Acronis

acronis.com

Cyber Protection

24.04

Podręcznik użytkownika

WERSJA: 09.05.2024

Spis treści

Rozpoczęcie pracy z produktem Cyber Protection ... 19
Aktywacja konta ... 19
Wymagania dotyczące hasła ... 19
Uwierzytelnianie dwuskładnikowe ... 19
Ustawienia ochrony prywatności ... 21
Uzyskiwanie dostępu do usługi Cyber Protection ... 22
Wymagania dotyczące oprogramowania ... 23
Obsługiwane przeglądarki internetowe ... 23
Obsługiwane systemy operacyjne i środowiska ... 23
Obsługiwane wersje programu Microsoft SQL Server ... 30
Obsługiwane wersje programu Microsoft Exchange Server ... 31
Obsługiwane wersje programu Microsoft SharePoint ... 31
Obsługiwane wersje systemu Oracle Database ... 31
Obsługiwane wersje platformy SAP HANA ... 32
Obsługiwane wersje programu MySQL ... 32
Obsługiwane wersje systemu MariaDB ... 32
Obsługiwane platformy wirtualizacji ... 32
Kompatybilność z programami szyfrującymi ... 44
Kompatybilność z urządzeniami pamięci masowej Dell EMC Data Domain ... 45
Obsługa funkcji ochrony w poszczególnych systemach operacyjnych ... 47
Obsługiwane systemy operacyjne i wersje ... 47
Obsługiwane systemy plików ... 57
Obsługiwane operacje na woluminach logicznych ... 61
Kopia zapasowa ... 61
Odzyskiwanie ... 62
Instalowanie i wdrażanie agentów Cyber Protection ... 63
Zanim zaczniesz ... 63
Przygotowanie ... 63
Tworzenie kopii zapasowych przy użyciu agenta i bezagentowe ... 66
Który agent jest potrzebny? ... 67
Wymagania systemowe agentów ... 71
Pobieranie agentów ochrony ... 74
Pakiety systemu Linux ... 74
Konfigurowanie ustawień serwera proxy ... 78
Dynamiczna instalacja i dezinstalacja komponentów ... 82

© Acronis International GmbH, 2003-2024

Przyznawanie wymaganych uprawnień systemowych modułowi Agent rozwiązania Connect 83
Instalowanie agentów ochrony przy użyciu graficznego interfejsu użytkownika 84
Instalowanie agentów ochrony w systemie Windows 84
Instalowanie agentów ochrony w systemie Linux 87
Instalowanie agentów ochrony w systemie macOS 89
Odinstalowywanie agentów 90
Instalowanie i odinstalowywanie agentów ochrony przy użyciu interfejsu wiersza polecenia 92
Instalowanie i odinstalowywanie agentów ochrony w systemie Windows 92
Przykłady 93
Przykład 94
Przykłady 94
Przykłady 102
Przykład 104
Przykłady 104
Instalowanie i odinstalowywanie agentów ochrony w systemie Linux 110
Instalowanie i odinstalowywanie agentów ochrony w systemie macOS 116
Rejestracja maszyn 127
Rejestrowanie maszyn przy użyciu graficznego interfejsu użytkownika 127
Rejestrowanie i wyrejestrowywanie maszyn przy użyciu interfejsu wiersza polecenia 132
Zmiana rejestracji obciążenia 137
Przenoszenie maszyn do innego dzierżawcy 137
Aktualizowanie agentów ochrony 137
Ręczne aktualizowanie agentów ochrony 138
Automatyczne aktualizowanie agentów ochrony 140
Aktualizowanie agentów ochrony na maszynach zaszyfrowanych przy użyciu funkcji BitLocker 142
Wdrażanie agentów ochrony przy użyciu zasad grupy 143
Wymagania wstępne 143
Tworzenie pliku transformacji i wyodrębnianie pakietów instalacyjnych 144
Konfigurowanie obiektu zasad grupy 144
Wdrażanie urządzeń wirtualnych 146
Wdrażanie agenta dla VMware (urządzenie wirtualne) 146
Wdrażanie agenta dla Scale Computing HC3 (urządzenie wirtualne) 150
Wdrażanie agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne) 155
Wdrażanie agenta dla oVirt (urządzenie wirtualne) 164
Wdrażanie agenta dla Synology 170
Połączenia SSH z urządzeniem wirtualnym 179
Automatyczne wykrywanie komputerów 181

© Acronis International GmbH, 2003-2024

Jak działa wykrywanie automatyczne ... 181
Jak działa zdalna instalacja agentów ... 183
Wykonywanie automatycznego i ręcznego wykrywania ... 183
Zarządzanie wykrytymi komputerami ... 190
Rozwiązywanie problemów ... 191
Zapobieganie nieuprawnionym dezinstalacjom lub modyfikacjom agentów ... 192
Zmienianie limitów usług komputerów ... 193
Ustawienia ochrony ... 195
Automatyczne aktualizacje komponentów ... 195
Aktualizowanie definicji Cyber Protection według harmonogramu ... 196
Aktualizowanie definicji Cyber Protection na żądanie ... 196
Pamięć podręczna ... 197
Usługi Cyber Protection instalowane w danym środowisku ... 197
Usługi instalowane w systemie Windows ... 197
Usługi instalowane w systemie macOS ... 198
Zapisywanie pliku dziennika agenta ... 198
Połączenie Open VPN site-to-site — dodatkowe informacje ... 198
Zarządzanie licencjami dla lokalnych serwerów zarządzania ... 206
Praca z planami ... 207
Opis planów ... 207
Plany wbudowane ... 208
Plany domyślne ... 217
Ulubione plany ... 219
Plany ochrony i moduły ... 221
Tworzenie planu ochrony ... 222
Czynności dotyczące planów ochrony ... 224
Usuwanie konfliktów między planami ... 228
Indywidualne plany ochrony do hostingu integracji panelu kontrolnego ... 229
Plany ochrony danych poza hostem ... 230
Replikacja kopii zapasowej ... 230
Sprawdzanie poprawności ... 234
Czyszczenie ... 242
Konwersja na maszynę wirtualną ... 243
Plany skanowania kopii zapasowych ... 247
Plany tworzenia kopii zapasowych aplikacji w chmurze ... 248
Ochrona aplikacji do współpracy i komunikacji ... 249
Poznanie bieżącego poziomu ochrony ... 251

© Acronis International GmbH, 2003-2024

Monitorowanie ... 251
Pulpit nawigacyjny Przegląd ... 251
Pulpit nawigacyjny Działania ... 252
Pulpit nawigacyjny Alerty ... 253
Typy alertów ... 254
Widżety alertów ... 276
Cyber Protection ... 277
Status ochrony ... 277
Widżety pakietu Endpoint Detection and Response (EDR) ... 279
Wynik #CyberFit według komputerów ... 283
Monitorowanie kondycji dysków ... 284
Mapa ochrony danych ... 288
Widżety dotyczące oceny luk w zabezpieczeniach ... 289
Widżety dotyczące instalacji poprawek ... 291
Szczegóły skanowania kopii zapasowej ... 292
Ostatnio dotknięte problemem ... 293
Aplikacje w chmurze ... 293
Widżet inwentaryzacji oprogramowania ... 294
Widżety inwentaryzacji sprzętu ... 295
Widżet Sesje zdalne ... 296
Inteligentna ochrona ... 297
Karta Działania ... 304
Cyber Protect Monitor ... 305
Konfigurowanie ustawień serwera proxy w narzędziu Cyber Protect Monitor ... 307
Raporty ... 307
Czynności dotyczące raportów ... 308
Raportowane dane zależnie od typu widżetu ... 310
Zarządzanie obciążeniami w konsoli Cyber Protect ... 313
Konsola Cyber Protect ... 313
Co nowego w konsoli Cyber Protect ... 314
Korzystanie z konsoli Cyber Protect w przypadku administratora partnera ... 315
Wymagania wstępne ... 319
Obciążenia ... 323
Dodawanie obciążeń do konsoli Cyber Protect ... 325
Usuwanie obciążeń z konsoli Cyber Protect ... 330
Grupy urządzeń ... 334
Grupy wbudowane i grupy niestandardowe ... 334

© Acronis International GmbH, 2003-2024

Grupy statyczne i grupy dynamiczne ... 335
Grupy międzychmurowe i inne niż międzychmurowe ... 336
Tworzenie grupy statycznej ... 336
Dodawanie obciążeń do grupy statycznej ... 338
Tworzenie grupy dynamicznej ... 339
Edytowanie grupy dynamicznej ... 357
Usuwanie grupy ... 358
Stosowanie planu do grupy ... 358
Odwoływanie planu z grupy ... 359
Korzystanie z modułu kontroli urządzeń ... 360
Korzystanie z kontroli urządzeń ... 363
Ustawienia dostępu ... 369
Lista dozwolonych typów urządzeń ... 375
Lista dozwolonych urządzeń USB ... 377
Wykluczanie procesów z kontroli dostępu ... 381
Alerty związane z kontrolą urządzeń ... 383
Wymazywanie danych z zarządzanego obciążenia ... 387
Obciążenia CyberApp ... 388
Obciążenia zagregowane ... 388
Praca z obciążeniami CyberApp ... 388
Praca z obciążeniami zagregowanymi ... 389
Znajdź ostatniego zalogowanego użytkownika ... 390
Wynik #CyberFit komputerów ... 391
Sposób działania ... 392
Uruchamianie skanowania w celu ustalenia wyniku #CyberFit ... 397
Skrypty cybernetyczne ... 398
Wymagania wstępne ... 399
Ograniczenia ... 399
Obsługiwane platformy ... 399
Role użytkowników a prawa do funkcji Skrypty cybernetyczne ... 400
Skrypty ... 402
Repozytorium skryptów ... 411
Plany skryptów ... 412
Szybkie uruchomienie skryptu ... 421
Zarządzanie tworzeniem kopii zapasowych oraz odzyskiwaniem obciążeń i plików ... 424
Kopia zapasowa ... 424
Plan ochrony — ściągawka ... 426

© Acronis International GmbH, 2003-2024

Wybieranie danych do uwzględnienia w kopii zapasowej ... 429
Wybieranie całego komputera ... 429
Wybieranie dysków lub woluminów ... 429
Wybieranie plików lub folderów ... 433
Wybieranie stanu systemu ... 436
Wybieranie konfiguracji ESXi ... 436
Ciągła ochrona danych ... 437
Sposób działania ... 437
Obsługiwane źródła danych ... 439
Obsługiwane lokalizacje docelowe ... 440
Konfigurowanie operacji tworzenia kopii zapasowych CDP ... 440
Wybieranie miejsca docelowego ... 441
Zaawansowana opcja magazynu ... 442
Secure Zone — informacje ... 443
Harmonogram tworzenia kopii zapasowych ... 446
Schematy tworzenia kopii zapasowych ... 447
Typy kopii zapasowych ... 449
Uruchamianie operacji tworzenia kopii zapasowej zgodnie z harmonogramem ... 450
Ręczne uruchamianie operacji tworzenia kopii zapasowej ... 466
Reguły przechowywania ... 467
Ważne wskazówki ... 467
Reguły przechowywania zgodnie ze schematem tworzenia kopii zapasowych ... 468
Konfigurowanie reguł przechowywania ... 471
Replikacja ... 472
Przykłady użycia ... 472
Obsługiwane lokalizacje ... 473
Szyfrowanie ... 474
Konfigurowanie szyfrowania w planie ochrony ... 474
Konfigurowanie szyfrowania jako właściwości komputera ... 475
Notaryzacja ... 477
Jak korzystać z funkcji notaryzacji ... 477
Sposób działania ... 478
Domyślne opcje tworzenia kopii zapasowej ... 478
Opcje tworzenia kopii zapasowych ... 479
Dostępne opcje tworzenia kopii zapasowych ... 479
Alerty ... 482
Konsolidacja kopii zapasowych ... 482

© Acronis International GmbH, 2003-2024

Nazwa pliku kopii zapasowej ... 483
Format kopii zapasowej ... 488
Sprawdzanie poprawności kopii zapasowej ... 489
CBT (Changed Block Tracking) ... 490
Tryb tworzenia kopii zapasowych klastra ... 490
Stopień kompresji ... 492
Obsługa błędów ... 492
Szybka przyrostowa/różnicowa kopia zapasowa ... 494
Filtry plików (uwzględniające/wykluczające) ... 494
Migawka kopii zapasowej na poziomie plików ... 496
Dane do analizy śledczej ... 496
Obcinanie dziennika ... 506
Wykonywanie migawek LVM ... 506
Punkty zamontowania ... 507
Migawka wielowoluminowa ... 508
Odzyskiwanie jednym kliknięciem ... 508
Wydajność i okno na utworzenie kopii zapasowej ... 513
Fizyczne dostarczanie danych ... 517
Polecenia poprzedzające/następujące ... 519
Polecenia poprzedzające rejestrowanie danych/następujące po nim ... 521
Tworzenie harmonogramu ... 524
Kopia zapasowa sektor po sektorze ... 525
Dzielenie ... 525
Obsługa niepowodzenia zadania ... 526
Warunki uruchomienia zadania ... 526
Usługa kopiowania woluminów w tle (VSS) ... 527
Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych ... 529
Tygodniowa kopia zapasowa ... 531
Dziennik zdarzeń systemu Windows ... 531
Odzyskiwanie ... 532
Odzyskiwanie — ściągawka ... 532
Bezpieczne odzyskiwanie ... 535
Odzyskiwanie komputera ... 536
Przygotuj sterowniki ... 546
Sprawdź dostęp do sterowników w środowisku startowym ... 547
Automatyczne wyszukiwanie sterowników ... 547
Sterowniki pamięci masowej do zainstalowania mimo to ... 547

© Acronis International GmbH, 2003-2024

Odzyskiwanie plików ... 549
Odzyskiwanie stanu systemu ... 556
Odzyskiwanie konfiguracji ESXi ... 557
Opcje odzyskiwania ... 558
Operacje dotyczące kopii zapasowych ... 566
Karta Magazyn kopii zapasowych ... 566
Montowanie woluminów z kopii zapasowej ... 568
Sprawdzanie poprawności kopii zapasowych ... 570
Eksportowanie kopii zapasowych ... 571
Usuwanie kopii zapasowych ... 572
Opis wykrywania wąskich gardeł ... 574
Tworzenie kopii zapasowych obciążeń w chmurach publicznych ... 579
Definiowanie lokalizacji kopii zapasowych na platformie Microsoft Azure ... 579
Definiowanie lokalizacji kopii zapasowych na platformie Amazon S3 ... 582
Definiowanie lokalizacji kopii zapasowych na platformie Wasabi ... 584
Wyświetlanie i aktualizowanie lokalizacji kopii zapasowych w chmurze publicznej ... 586
Zarządzanie dostępem do kont w chmurze publicznej ... 587
Ochrona aplikacji firmy Microsoft ... 599
Chronienie programów Microsoft SQL Server i Microsoft Exchange Server ... 599
Ochrona programu Microsoft SharePoint ... 599
Chronienie kontrolera domeny ... 600
Odzyskiwanie aplikacji ... 600
Wymagania wstępne ... 601
Kopia zapasowa bazy danych ... 603
Kopia zapasowa uwzględniająca aplikacje ... 609
Kopia zapasowa skrzynki pocztowej ... 612
Odzyskiwanie baz danych SQL ... 614
Odzyskiwanie baz danych programu Exchange ... 623
Odzyskiwanie skrzynek pocztowych programu Exchange i ich elementów ... 626
Zmiana poświadczeń dostępu programu SQL Server lub Exchange Serwer ... 633
Ochrona urządzeń mobilnych ... 633
Obsługiwane urządzenia mobilne ... 633
Elementy, które można uwzględnić w kopii zapasowej ... 634
Co trzeba wiedzieć ... 634
Jak uzyskać aplikację Cyber Protect ... 635
Jak rozpocząć tworzenie kopii zapasowej danych ... 635
Jak odzyskać dane na urządzenie mobilne ... 635

© Acronis International GmbH, 2003-2024

Jak przeglądać dane za pomocą konsoli Cyber Protect ... 636
Chronienie danych usługi Hosted Exchange ... 637
Jakie elementy można uwzględnić w kopii zapasowej? ... 637
Jakie elementy można odzyskać? ... 637
Wybieranie skrzynek pocztowych programu Exchange Online ... 638
Odzyskiwanie skrzynek pocztowych i elementów skrzynek pocztowych ... 639
Ochrona danych Microsoft 365 ... 641
Dlaczego warto tworzyć kopie zapasowe danych Microsoft 365? ... 641
Agent w chmurze i agent lokalny ... 641
Wymagane prawa użytkownika ... 644
Ograniczenia ... 645
Raport o licencjonowaniu stanowisk Microsoft 365 ... 646
Prowadzenie dziennika ... 646
Korzystanie z zainstalowanego lokalnie agenta dla Office 365 ... 647
Przy użyciu chmurowego agenta dla usługi Microsoft 365 ... 651
Ochrona danych pakietu Google Workspace ... 686
Co oznacza ochrona danych pakietu Google Workspace? ... 686
Wymagane prawa użytkownika ... 687
Informacje o harmonogramie tworzenia kopii zapasowych ... 687
Ograniczenia ... 688
Prowadzenie dziennika ... 688
Dodawanie organizacji Google Workspace ... 688
Tworzenie osobistego projektu Google Cloud ... 689
Wykrywanie zasobów z usługi Google Workspace ... 693
Ustawianie częstotliwości tworzenia kopii zapasowych danych Google Workspace ... 694
Ochrona danych rozwiązania Gmail ... 695
Ochrona plików z Dysku Google ... 699
Ochrona plików z Dysku udostępnionego ... 703
Notaryzacja ... 708
Wyszukiwanie w kopiach zapasowych z chmury do chmury ... 709
Wyszukiwanie pełnotekstowe ... 709
Indeksy wyszukiwania ... 710
Sprawdzanie rozmiaru indeksu wyszukiwania ... 710
Aktualizowanie, odbudowywanie lub usuwanie indeksów ... 710
Wyłączanie wyszukiwania pełnotekstowego w przypadku kopii zapasowych usługi Gmail ... 712
Ochrona systemu Oracle Database ... 712
Ochrona platformy SAP HANA ... 712

© Acronis International GmbH, 2003-2024

Chronienie danych z baz MySQL i MariaDB ... 713
Konfigurowanie kopii zapasowej uwzględniającej aplikacje ... 714
Odzyskiwanie danych z kopii zapasowej uwzględniającej aplikacje ... 715
Ochrona witryn internetowych i serwerów hostingu ... 720
Ochrona witryn internetowych ... 720
Ochrona serwerów hostingu witryn internetowych ... 723
Specjalne operacje dotyczące maszyn wirtualnych ... 724
Uruchamianie maszyny wirtualnej z kopii zapasowej (Instant Restore) ... 724
Praca w środowisku VMware vSphere ... 729
Tworzenie kopii zapasowych maszyn Hyper-V w klastrach ... 752
Ograniczanie łącznej liczby maszyn wirtualnych, których kopie zapasowe mogą być tworzone w tym samym czasie ... 753
Migracja komputera ... 754
Maszyny wirtualne Microsoft Azure i Amazon EC2 ... 759
Tworzenie nośników startowych do odzyskiwania systemów operacyjnych ... 759
Niestandardowy czy gotowy nośnik startowy? ... 759
Nośnik startowy oparty na systemie Linux czy na środowisku WinPE/WinRE? ... 760
Tworzenie fizycznego nośnika startowego ... 761
Generator nośnika startowego ... 762
Odzyskiwanie z magazynu w chmurze ... 766
Odzyskiwanie z udziału sieciowego ... 766
Pliki skryptu ... 767
Struktura pliku autostart.json ... 767
Obiekt najwyższego poziomu ... 767
Obiekt zmiennej ... 768
Typ elementu sterującego ... 769
Nawiązywanie połączenia z komputerem uruchomionym z nośnika startowego ... 777
Lokalne operacje wykonywane przy użyciu nośnika startowego ... 777
Operacje zdalne dotyczące nośnika startowego ... 779
Startup Recovery Manager ... 782
Wdrażanie funkcji odzyskiwania po awarii ... 786
Cyber Disaster Recovery Cloud — informacje ... 786
Najważniejsze funkcje ... 786
Wymagania dotyczące oprogramowania ... 787
Obsługiwane systemy operacyjne ... 787
Obsługiwane platformy wirtualizacji ... 787
Ograniczenia ... 788

© Acronis International GmbH, 2003-2024

Wersja próbna rozwiązania Cyber Disaster Recovery Cloud ... 790
Ograniczenia w przypadku korzystania z magazynu Geo-redundant Cloud Storage ... 790
Kompatybilność modułu Odzyskiwanie po awarii z programami szyfrującymi ... 790
Punkty obliczeniowe ... 791
Konfigurowanie funkcji odzyskiwania po awarii ... 792
Tworzenie planu ochrony na potrzeby odzyskiwania po awarii ... 793
Edytowanie domyślnych parametrów serwera odzyskiwania ... 795
Infrastruktura sieci w chmurze ... 796
Konfigurowanie łączności ... 797
Pojęcia dotyczące sieci ... 797
Początkowa konfiguracja łączności ... 808
Wymagania wstępne ... 811
Zarządzanie sieciami ... 818
Wymagania wstępne ... 834
Konfigurowanie serwerów odzyskiwania ... 835
Tworzenie serwera odzyskiwania ... 835
Przebieg przełączania awaryjnego ... 838
Przebieg powrotu po awarii ... 847
Wymagania wstępne ... 849
Wymagania wstępne ... 854
Praca z zaszyfrowanymi kopiami zapasowymi ... 858
Operacje dotyczące maszyn wirtualnych Microsoft Azure ... 859
Konfigurowanie serwerów podstawowych ... 859
Tworzenie serwera podstawowego ... 859
Działania na serwerze podstawowym ... 862
Zarządzanie serwerami chmurowymi ... 862
Reguły zapory dotyczące serwerów chmurowych ... 863
Ustawianie reguł zapory dla serwerów chmurowych ... 864
Sprawdzanie działań dotyczących zapory chmury ... 867
Tworzenie kopii zapasowych serwerów chmurowych ... 867
Orkiestracja (runbooki) ... 868
Dlaczego warto korzystać z runbooków? ... 868
Tworzenie runbooka ... 868
Operacje przy użyciu runbooków ... 872
Konfigurowanie ochrony przed wirusami i złośliwym oprogramowaniem ... 875
Obsługiwane platformy ... 875
Obsługiwane funkcje na platformach ... 876

© Acronis International GmbH, 2003-2024

Ochrona przed wirusami i złośliwym oprogramowaniem ... 879
Funkcje antywirusowe ... 879
Typy skanowania ... 880
Ustawienia modułu Ochrona przed wirusami i złośliwym oprogramowaniem ... 881
Active Protection w wersji Cyber Backup Standard ... 898
Ustawienia usługi Active Protection w oprogramowaniu Cyber Backup Standard ... 898
Filtrowanie adresów URL ... 906
Sposób działania ... 906
Proces konfiguracji modułu Filtrowanie adresów URL ... 908
Ustawienia modułu Filtrowanie adresów URL ... 908
Opis ... 915
Oprogramowanie Microsoft Defender Antivirus i Microsoft Security Essentials ... 915
Zaplanuj skanowanie ... 916
Czynności domyślne ... 916
Ochrona w czasie rzeczywistym ... 917
Zaawansowany ... 917
Wykluczenia ... 918
Zarządzanie zaporą ... 918
Kwarantanna ... 919
Jak pliki trafiają do folderu kwarantanny? ... 920
Zarządzanie plikami poddanymi kwarantannie ... 920
Lokalizacja kwarantanny na komputerach ... 921
Samoobsługowy niestandardowy folder na żądanie ... 921
Firmowa biała lista ... 921
Automatyczne dodawanie pozycji do białej listy ... 922
Ręczne dodawanie pozycji do białej listy ... 922
Dodawanie plików poddanych kwarantannie do białej listy ... 922
Ustawienia białej listy ... 922
Wyświetlanie szczegółowych informacji na temat pozycji z białej listy ... 923
Skanowanie antywirusowe kopii zapasowych ... 923
Ograniczenia ... 924
Korzystanie z funkcji ochrony zaawansowanej ... 926
Advanced Data Loss Prevention ... 928
Tworzenie zasad i reguł przepływów danych ... 928
Włączanie modułu Advanced Data Loss Prevention w planach ochrony ... 938
Automatyczne wykrywanie miejsca docelowego ... 942
Definicje poufnych danych ... 943

© Acronis International GmbH, 2003-2024

Zdarzenia funkcji Zapobieganie utracie danych ... 949
Widżety usługi Advanced Data Loss Prevention na pulpicie nawigacyjnym Przegląd ... 951
Niestandardowe kategorie poufności ... 952
Mapa organizacji ... 954
Znane problemy i ograniczenia ... 957
Endpoint Detection and Response (EDR) ... 957
Dlaczego potrzebne jest rozwiązanie Endpoint Detection and Response (EDR) ... 958
Włączanie funkcji modułu Endpoint Detection and Response (EDR) ... 961
Korzystanie z modułu pakietu Endpoint Detection and Response (EDR) ... 963
Wyświetlanie incydentów, których skutków jeszcze nie zniwelowano ... 967
Ustalanie zakresu i skutków incydentów ... 968
Składnia ... 972
Przykładowe zapytania ... 974
Typy i pola zdarzeń ... 975
Typy zdarzeń ... 975
Przykładowe typy danych ... 976
Pola zdarzeń ... 977
Jak się poruszać po etapach ataku ... 991
Włączanie trybu monitorowania dla modułu Endpoint Detection and Response (EDR) ... 1029
Sprawdzanie, czy pakiet Endpoint Detection and Response (EDR) poprawnie działa ... 1031
Ocena luk w zabezpieczeniach i zarządzanie poprawkami ... 1034
Ocena luk w zabezpieczeniach ... 1034
Obsługiwane produkty firmy Microsoft i innych firm ... 1035
Obsługiwane produkty firmy Apple i innych firm ... 1036
Obsługiwane produkty dla systemu Linux ... 1037
Ustawienia modułu Ocena luk w zabezpieczeniach ... 1037
Ocena luk w zabezpieczeniach komputerów z systemem Windows ... 1040
Ocena luk w zabezpieczeniach w przypadku komputerów z systemem Linux ... 1041
Ocena luk w zabezpieczeniach urządzeń z systemem macOS ... 1041
Zarządzanie znalezionymi lukami w zabezpieczeniach ... 1042
Zarządzanie poprawkami ... 1044
Przepływ pracy zarządzania poprawkami ... 1044
Ustawienia zarządzania poprawkami w planie ochrony ... 1045
Wyświetlanie listy dostępnych poprawek ... 1051
Automatyczne zatwierdzanie poprawek ... 1053
Ręczne zatwierdzanie poprawek ... 1058
Instalowanie poprawek na żądanie ... 1058

© Acronis International GmbH, 2003-2024

Zarządzanie inwentaryzacją oprogramowania i sprzętu **1061**
Inwentaryzacja oprogramowania 1061
Włączanie skanowania w celu inwentaryzacji oprogramowania 1061
Ręczne uruchamianie skanowania w celu inwentaryzacji oprogramowania 1062
Przeglądanie wyników inwentaryzacji oprogramowania 1062
Wyświetlanie wyników inwentaryzacji oprogramowania wybranego urządzenia 1064
Inwentaryzacja sprzętu 1065
Włączanie skanowania w celu inwentaryzacji sprzętu 1066
Ręczne uruchamianie skanowania w celu inwentaryzacji sprzętu 1067
Przeglądanie wyników inwentaryzacji sprzętu 1067
Wyświetlanie sprzętu wybranego urządzenia 1070
Nawiązywanie połączeń z zarządzanymi obciążeniami na potrzeby pulpitu zdalnego lub pomocy zdalnej **1072**
Obsługiwane funkcje pulpitu zdalnego i pomocy zdalnej 1074
Obsługiwane platformy 1077
Protokoły połączeń zdalnych 1078
NEAR 1078
RDP 1080
Udostępnianie ekranu firmy Apple 1080
Przekierowanie dźwięku w ramach połączenia zdalnego 1080
Połączenia z obciążeniami zdalnymi na potrzeby pulpitu zdalnego lub pomocy zdalnej 1081
Plany zarządzania zdalnego 1082
Tworzenie planu zarządzania zdalnego 1083
Dodawanie obciążenia do planu zarządzania zdalnego 1091
Usuwanie obciążeń z planu zarządzania zdalnego 1092
Dodatkowe czynności w ramach istniejących już planów zarządzania zdalnego 1092
Problemy z kompatybilnością z planami zarządzania zdalnego 1095
Rozwiązywanie problemów z kompatybilnością z planami zarządzania zdalnego 1096
Poświadczenia dostępu do obciążenia 1097
Dodawanie poświadczeń 1098
Przypisywanie poświadczeń do obciążenia 1099
Usuwanie poświadczeń 1099
Cofanie przypisania poświadczeń z obciążenia 1099
Praca z obciążeniami zarządzanymi 1100
Konfigurowanie ustawień protokołu RDP 1100
Nawiązywanie połączeń z obciążeniami zarządzanymi na potrzeby pulpitu zdalnego lub pomocy zdalnej 1101

© Acronis International GmbH, 2003-2024

Nawiązywanie połączenia z obciążeniem zarządzanym przy użyciu klienta internetowego 1104
Przesyłanie plików 1105
Wykonywanie czynności związanych ze sterowaniem na obciążeniach zarządzanych 1106
Monitorowanie obciążeń przy użyciu funkcji przesyłania zrzutów ekranu 1107
Obserwowanie wielu obciążeń zarządzanych naraz 1108
Praca z obciążeniami niezarządzanymi 1110
Nawiązywanie połączeń z obciążeniami niezarządzanymi przy użyciu aplikacji Acronis Quick Assist 1110
Nawiązywanie połączeń z obciążeniami niezarządzanymi przy użyciu adresów IP 1111
Przesyłanie plików za pośrednictwem aplikacji Acronis Quick Assist 1112
Korzystanie z paska narzędzi w oknie podglądu 1113
Nagrywanie i odtwarzanie sesji zdalnych 1116
Konfigurowanie ustawień programu Klient rozwiązania Connect 1117
Powiadomienia dotyczące pulpitu zdalnego 1118
Monitorowanie kondycji i wydajności obciążeń 1120
Plany monitorowania 1120
Typy monitorowania 1120
Monitorowanie typu Wykrywanie anomalii 1121
Platformy obsługiwane w ramach monitorowania 1121
Konfigurowalne monitory 1121
Ustawienia monitora Miejsce na dysku 1127
Ustawienia monitora Temperatura procesora 1130
Ustawienia monitora Temperatura procesora graficznego 1131
Ustawienia monitora Zmiany sprzętowe 1133
Ustawienia monitora Poziom użycia procesora 1133
Ustawienia monitora Poziom użycia pamięci 1135
Ustawienia monitora Szybkość transferu dysku 1137
Ustawienia monitora Wykorzystanie sieci 1140
Ustawienia monitora Poziom użycia procesora przez proces 1143
Ustawienia monitora Poziom użycia pamięci przez proces 1144
Ustawienia monitora Szybkość transferu dysku generowanego przez proces 1145
Ustawienia monitora Poziom użycia sieci przez proces 1146
Ustawienia monitora Status usług systemu Windows 1147
Ustawienia monitora Status procesu 1148
Ustawienia monitora Zainstalowane oprogramowanie 1148
Ustawienia monitora Ostatnie ponowne uruchomienie systemu 1149
Ustawienia monitora Dziennik zdarzeń systemu Windows 1150

© Acronis International GmbH, 2003-2024

Ustawienia monitora Rozmiar plików i folderów ... 1151
Ustawienia monitora Status usługi Windows Update ... 1152
Ustawienia monitora Status zapory ... 1152
Ustawienia monitora Niepowodzenia logowania ... 1152
Ustawienia monitora Status oprogramowania antywirusowego ... 1153
Ustawienia monitora Status funkcji uruchamiania automatycznego ... 1155
Ustawienia monitora Niestandardowe ... 1155
Plany monitorowania ... 1156
Tworzenie planu monitorowania ... 1157
Dodawanie obciążeń do planów monitorowania ... 1159
Odwoływanie planów monitorowania ... 1160
Konfigurowanie automatycznych czynności w ramach reagowania ... 1160
Dodatkowe czynności dotyczące planów monitorowania ... 1162
Problemy z kompatybilnością dotyczące planów monitorowania ... 1166
Rozwiązywanie problemów z kompatybilnością dotyczących planów monitorowania ... 1166
Resetowanie modeli uczenia maszynowego ... 1167
Alerty dotyczące monitorowania ... 1168
Konfigurowanie alertów dotyczących monitorowania ... 1168
Zmienne alertów dotyczących monitorowania ... 1169
Ręczne czynności w ramach reagowania ... 1172
Wyświetlanie alertów z monitorowania dotyczących wybranego obciążenia ... 1175
Wyświetlanie dziennika alertów dotyczących monitorowania ... 1175
Konfigurowanie zasad powiadamiania pocztą e-mail ... 1176
Wyświetlanie danych z monitora ... 1177
Widżety monitorów ... 1178
Dodatkowe narzędzia Cyber Protection ... 1180
Tryb zgodności ... 1180
Ograniczenia ... 1180
Nieobsługiwane funkcje ... 1180
Ustawianie hasła szyfrowania ... 1181
Zmienianie hasła szyfrowania ... 1181
Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności ... 1182
Niezmienny magazyn ... 1182
Tryby niezmiennego magazynu ... 1182
Obsługiwane magazyny i agenty ... 1183
Włączanie niezmiennego magazynu ... 1183
Wyłączanie niezmiennego magazynu ... 1184

© Acronis International GmbH, 2003-2024

Uzyskiwanie dostępu do usuniętych kopii zapasowych w niezmiennym magazynie 1184
Magazyn z geograficzną nadmiarowością 1185
Włączanie i wyłączanie magazynu z geograficzną nadmiarowością 1185
Status georeplikacji 1186
Ograniczenia 1186
Słownik **1187**
Indeks **1192**

© Acronis International GmbH, 2003-2024

Rozpoczęcie pracy z produktem Cyber Protection

Aktywacja konta

Gdy administrator utworzy Twoje konto, na Twój adres e-mail zostanie wysłana wiadomość. Wiadomość ta zawiera następujące informacje:

- **Nazwa logowania.** Nazwa użytkownika, której używasz do logowania się. Nazwa logowania jest też widoczna na stronie aktywacji konta.
- Przycisk **Aktywuj konto**. Kliknij ten przycisk i ustaw hasło do konta. Hasło musi się składać z co najmniej dziewięciu znaków. Dodatkowe informacje na temat hasła można znaleźć w sekcji "Wymagania dotyczące hasła" (s. 19).

Jeśli administrator włączył uwierzytelnianie dwuskładnikowe, pojawi się monit o skonfigurowanie takiego uwierzytelniania na koncie. Dodatkowe informacje na ten temat można znaleźć w sekcji "Uwierzytelnianie dwuskładnikowe" (s. 19).

Wymagania dotyczące hasła

Hasło do konta użytkownika musi się składać z co najmniej 9 znaków. Hasła są też sprawdzane pod kątem złożoności i oceniane przy użyciu jednej z następujących kategorii:

- Słabe
- Średni
- Silne

Nie można zapisać słabego hasła, nawet jeśli składa się ono z 9 lub większej liczby znaków. Hasła, w których jest powtarzana nazwa użytkownika, nazwa logowania, adres e-mail użytkownika lub nazwa dzierżawcy, do którego przynależy konto użytkownika, są zawsze uważane za słabe. Za słabe też uznaje się najpopularniejsze hasła.

Aby zwiększyć siłę hasła, należy dodać do niego kolejne znaki. Stosowanie różnych rodzajów znaków, na przykład cyfr, małych i wielkich liter oraz znaków specjalnych, nie jest konieczne, ale pozwala uzyskać większą siłę hasła przy mniejszej liczbie znaków.

Uwierzytelnianie dwuskładnikowe

Uwierzytelnianie dwuskładnikowe (two-factor authentication, 2FA) zapewnia dodatkową ochronę przed nieuprawnionym dostępem do konta. Jeśli zostało skonfigurowane uwierzytelnianie dwuskładnikowe, w celu zalogowania się do konsoli Cyber Protect trzeba podać hasło (pierwszy składnik) i jednorazowy kod (drugi składnik). Jednorazowy kod jest generowany przez specjalną aplikację, która musi być zainstalowana na telefonie komórkowym lub innym urządzeniu. Nawet

© Acronis International GmbH, 2003-2024

jeśli ktoś pozna nazwę logowania i hasło, bez dostępu do urządzenia obsługującego drugi składnik uwierzytelniania wciąż nie będzie mógł się zalogować na Twoim koncie.

Aby skonfigurować uwierzytelnianie dwuskładnikowe na koncie

Jeśli administrator włączył uwierzytelnianie dwuskładnikowe dla Twojej organizacji, musisz je skonfigurować dla swojego konta. Jeśli administrator włączy uwierzytelnianie dwuskładnikowe w czasie Twojego zalogowania się na konsoli Cyber Protect, trzeba będzie je skonfigurować po wygaśnięciu tej sesji.

Wymagania wstępne

- Uwierzytelnianie dwuskładnikowe zostało włączone przez administratora dla organizacji.

Aby skonfigurować uwierzytelnianie dwuskładnikowe na koncie

1. Zainstaluj aplikację uwierzytelniającą na urządzeniu mobilnym.
   Przykłady aplikacji uwierzytelniających:
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. Zeskanuj kod QR za pomocą aplikacji uwierzytelniającej, a następnie wprowadź 6-cyfrowy kod wyświetlany w aplikacji uwierzytelniającej w oknie **Skonfiguruj uwierzytelnianie dwuskładnikowe**.
3. Kliknij **Dalej**.
   Wyświetlane są instrukcje dotyczące przywracania dostępu do konta w przypadku utraty urządzenia używanego do uwierzytelniania dwuskładnikowego lub odinstalowania aplikacji uwierzytelniającej.
4. Zapisz lub wydrukuj plik PDF.

   Uwaga
   Koniecznie zapisz ten plik PDF w bezpiecznym miejscu lub wydrukuj w celu wykorzystania w przyszłości. Jest to najlepszy sposób na przywrócenie dostępu.

5. Wróć do strony logowania w konsoli Cyber Protect i wprowadź wygenerowany kod.
   Jednorazowy kod jest ważny przez 30 sekund. Jeśli upłynie więcej niż 30 sekund, użyj następnego wygenerowanego kodu.

Przy następnym logowaniu się możesz zaznaczyć pole wyboru **Ufaj tej przeglądarce**. Jeśli to zrobisz, przy następnych logowaniach się przy użyciu tej przeglądarki na tym komputerze nie trzeba już będzie podawać kodu.

Uwaga
Zalecamy pozostawienie tego pola wyboru bez zaznaczenia. W przeciwnym razie utracisz dostęp do uwierzytelniania dwuskładnikowego w przypadku swojego konta.

Aby przywrócić uwierzytelnianie dwuskładnikowe na nowym urządzeniu

© Acronis International GmbH, 2003-2024

Jeśli masz dostęp do wcześniej skonfigurowanej mobilnej aplikacji uwierzytelniającej

1. Zainstaluj aplikację uwierzytelniającą na nowym urządzeniu.
2. Skorzystaj z pliku PDF zapisanego podczas konfigurowania uwierzytelniania dwuskładnikowego na urządzeniu. Plik ten zawiera 32-cyfrowy kod, który trzeba podać w aplikacji uwierzytelniającej, aby ponownie nawiązać połączenie między aplikacją uwierzytelniającą i kontem Acronis.

   Ważne
   Jeśli kod nie działa, sprawdź, czy ustawienia czasu w mobilnej aplikacji uwierzytelniającej są zsynchronizowane z Twoim urządzeniem.

   Jeśli podczas konfiguracji nie zapisano pliku PDF:

a. Kliknij **Zresetuj uwierzytelnianie dwuskładnikowe**, a następnie wprowadź jednorazowe hasło wyświetlane w mobilnej aplikacji uwierzytelniającej.
b. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Jeśli nie masz dostępu do wcześniej skonfigurowanej mobilnej aplikacji uwierzytelniającej

1. Skorzystaj z nowego urządzenia mobilnego.
2. Użyj zapisanego pliku PDF (domyślna nazwa pliku to `cyberprotect-2fa-backupcode.pdf`), aby powiązać nowe urządzenie.
3. Przywróć dostęp do konta z poziomu kopii zapasowej. Upewnij się, że kopie zapasowe są obsługiwane przez używaną aplikację mobilną.
4. Otwórz aplikację na tym samym koncie z innego urządzenia mobilnego, jeśli jest ono obsługiwane przez aplikację.

Ustawienia ochrony prywatności

Ustawienia prywatności pomagają określić, czy wyrażasz zgodę na zbieranie, wykorzystywanie i ujawnianie Twoich danych osobowych.

W zależności od kraju, w którym korzystasz z usługi Cyber Protect Cloud, i centrum danych Cyber Protect Cloud, które świadczy usługi, przy pierwszym uruchomieniu usługi Cyber Protect Cloud może pojawić się prośba o potwierdzenie, że zgadzasz się na korzystanie z usługi Google Analytics w usłudze Cyber Protect Cloud.

Usługa Google Analytics pomaga nam lepiej zrozumieć zachowanie użytkowników i poprawić środowisko użytkownika usługi Cyber Protect Cloud dzięki zbieraniu pseudonimizowanych danych.

W przypadku włączenia lub odmowy włączenia usługi Google Analytics przy pierwszym uruchomieniu usługi Cyber Protect Cloud, możesz później zmienić tę decyzję w dowolnym momencie.

Aby włączyć lub wyłączyć usługę Google Analytics

1. W konsoli Cyber Protect kliknij **Zarządzaj kontem**.
2. Kliknij ikonę konta w prawym górnym rogu.

© Acronis International GmbH, 2003-2024

3. Wybierz **Moje ustawienia ochrony prywatności**. Zostanie wyświetlone okno **Moje ustawienia ochrony prywatności**.
4. W sekcji **Zbieranie danych przez narzędzie Google Analytics** kliknij jeden z następujących przycisków:
   - **Włącz**, aby włączyć usługę Google Analytics
   - **Wyłącz**, aby wyłączyć usługę Google Analytics

W sekcji **Jak usunąć pliki cookie** możesz kontrolować pliki cookie i zarządzać nimi bezpośrednio w przeglądarce.

Uwaga
Jeśli nie ma sekcji dotyczącej usługi Google Analytics, oznacza to, że usługa Google Analytics nie jest używana w Twoim kraju.

W sekcji **Pomoc interaktywna i wdrażanie w produkcie** widocznej na początku w okresie próbnym, można zatrzymać lub zachować otrzymywanie w przyszłości informacji o ulepszeniach i nowych funkcjach programu. Funkcja ta jest domyślnie włączona, ale można ją wyłączyć, przełączając przełącznik w pozycję **Wył**.

Uzyskiwanie dostępu do usługi Cyber Protection

Po aktywacji konta można uzyskać dostęp do usługi Cyber Protection przez zalogowanie się do konsoli Cyber Protect lub za pośrednictwem portalu zarządzania.

Aby się zalogować do konsoli Cyber Protect

1. Przejdź do strony logowania do usługi Cyber Protection.
2. Wpisz nazwę logowania i kliknij **Dalej**.
3. Wpisz hasło, a następnie kliknij **Dalej**.
4. [W przypadku korzystania z więcej niż jednej usługi Cyber Protect Cloud] Kliknij **Cyber Protection**.
   Użytkownicy, którzy mają dostęp tylko do usługi Cyber Protection, logują się bezpośrednio do konsoli Cyber Protect.
   Jeśli **Cyber Protection** nie jest jedyną usługą, do której masz dostęp, możesz przełączać między usługami za pomocą ikony dostępnej w prawym górnym rogu. Administratorzy mogą również za pomocą tej ikony przechodzić do portalu zarządzania.

Limit czasu użytkowania konsoli Cyber Protect wynosi 24 godziny w przypadku sesji aktywnych i 1 godzinę w przypadku sesji nieaktywnych.

Możesz zmienić język interfejsu internetowego, klikając ikonę konta w prawym górnym rogu.

Aby uzyskać dostęp do konsoli Cyber Protect z portalu zarządzania

© Acronis International GmbH, 2003-2024

1. W portalu zarządzania wybierz **Monitorowanie** > **Wykorzystanie**.
2. W obszarze **Cyber Protect** wybierz **Ochrona**, a następnie kliknij **Zarządzaj usługą**.
   Możesz też wybrać klienta w obszarze **Klienci**, a następnie kliknąć **Zarządzaj usługą**.

W wyniku tego nastąpi przekierowanie do konsoli Cyber Protect.

Ważne
Jeśli klient jest w trybie zarządzania **Samoobsługa**, nie można zarządzać usługami na jego rzecz. Tylko administratorzy klienta mogą zmienić tryb klienta na **Zarządzane przez dostawcę usługi**, a następnie zarządzać usługami.

Aby zresetować hasło

1. Przejdź do strony logowania do usługi Cyber Protection.
2. Wpisz nazwę logowania i kliknij **Dalej**.
3. Kliknij **Nie pamiętasz hasła?**.
4. Potwierdź, że chcesz otrzymać dodatkowe instrukcje, klikając **Wyślij**.
5. Postępuj zgodnie z instrukcjami zawartymi w otrzymanej wiadomości e-mail.
6. Skonfiguruj nowe hasło.

Wymagania dotyczące oprogramowania

Obsługiwane przeglądarki internetowe

Konsola Cyber Protect korzysta z protokołu TLS 1.2 i obsługuje następujące przeglądarki internetowe:

- Google Chrome 29 lub nowsza
- Mozilla Firefox 23 lub nowsza
- Opera 16 lub nowsza
- Microsoft Edge 25 lub nowsza
- Safari 8 lub nowsza w systemach operacyjnych macOS oraz iOS

W innych przeglądarkach internetowych (oraz w programie Safari działającym w innych systemach operacyjnych) interfejs użytkownika może być wyświetlany niepoprawnie lub niektóre funkcje mogą być niedostępne.

Obsługiwane systemy operacyjne i środowiska

Agent dla systemu Windows

Ten agent obejmuje komponent na potrzeby usług Ochrona przed wirusami i złośliwym oprogramowaniem oraz Filtrowanie adresów URL. Szczegółowe informacje na temat funkcji

© Acronis International GmbH, 2003-2024

obsługiwanych w systemach operacyjnych można znaleźć w sekcji "Obsługa funkcji ochrony w poszczególnych systemach operacyjnych" (s. 47).

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 lub nowszy — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008, Windows Server 2008 SP2* — wersje Standard, Enterprise, Datacenter, Foundation i Web (x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 — wszystkie wersje

Uwaga
Aby korzystać z rozwiązania Cyber Protection w połączeniu z systemem Windows 7, przed zainstalowaniem agenta ochrony trzeba zainstalować następujące aktualizacje od firmy Microsoft:

- Rozszerzone aktualizacje zabezpieczeń (ESU) systemu Windows 7
- KB4474419
- KB4490628

Więcej informacji na temat wymaganych aktualizacji można znaleźć w tym artykule bazy wiedzy Knowledge Base.

- Windows Server 2008 R2* — wersje Standard, Enterprise, Datacenter, Foundation i Web
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* — wszystkie wersje
- Windows 8/8.1 — wszystkie wersje (x86, x64) z wyjątkiem systemu Windows RT
- Windows Server 2012/2012 R2 — wszystkie wersje
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 — wersje Home, Pro, Education, Enterprise, IoT Enterprise i LTSC (dawniej LTSB)
- Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows 11 — wszystkie wersje
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

© Acronis International GmbH, 2003-2024

Uwaga

* Aby korzystać z rozwiązania Cyber Protection w tej wersji systemu Windows, przed zainstalowaniem agenta ochrony trzeba zainstalować aktualizację od firmy Microsoft dotyczącą obsługi podpisywania kodu przy użyciu algorytmu SHA2: KB4474419.

Dodatkowe informacje na temat problemów dotyczących aktualizacji z obsługą podpisywania kodu przy użyciu algorytmu SHA2 można znaleźć w tym artykule z bazy wiedzy Knowledge Base.

Agent dla SQL, agent dla usługi Active Directory, agent dla programu Exchange (na potrzeby kopii zapasowych baz danych oraz kopii zapasowych uwzględniających aplikacje)

Każdy z tych agentów można zainstalować na komputerze z dowolnym wymienionym wyżej systemem operacyjnym i obsługiwaną wersją odpowiedniej aplikacji.

Agent dla rozwiązania Data Loss Prevention

Kontrola urządzeń

- Microsoft Windows 7 Service Pack 1 lub nowszy
- Microsoft Windows Server 2008 R2 lub nowszy
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

Uwaga

Agent dla usługi Zapobieganie utracie danych przeznaczony dla systemu macOS obsługuje tylko procesory x64. Procesory Apple Silicon oparte na architekturze ARM nie są obsługiwane.

Zapobieganie utracie danych

- Microsoft Windows 7 Service Pack 1 lub nowszy
- Microsoft Windows Server 2008 R2 lub nowszy

Uwaga

Agenta dla usługi Zapobieganie utracie danych można instalować w nieobsługiwanych systemach macOS, ponieważ jest integralną częścią programu agenta dla systemu Mac. W takim przypadku w konsoli usługi Cyber Protect pojawi się informacja, że agent dla usługi Zapobieganie utracie danych jest zainstalowany na komputerze, ale funkcje kontroli urządzeń i zapobiegania utracie danych nie będą działać. Funkcja kontroli urządzeń będzie działać tylko w systemach macOS obsługiwanych przez agenta dla usługi Zapobieganie utracie danych.

© Acronis International GmbH, 2003-2024

Agent dla modułu Advanced Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 lub nowszy
- Microsoft Windows Server 2008 R2 lub nowszy

Agent dla systemu File Sync & Share

Listę obsługiwanych systemów operacyjnych można znaleźć w Podręczniku użytkownika rozwiązania Cyber Files Cloud.

Agent dla programu Exchange (na potrzeby kopii zapasowych skrzynek pocztowych)

- Windows Server 2008 — wersje Standard, Enterprise, Datacenter, Foundation i Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 — wszystkie wersje
- Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter, Foundation i Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 — wszystkie wersje
- Windows 8/8.1 — wszystkie wersje (x86, x64) z wyjątkiem systemu Windows RT
- Windows Server 2012/2012 R2 — wszystkie wersje
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 — wersje Home, Pro, Education i Enterprise
- Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows 11 — wszystkie wersje
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Agent dla usługi Microsoft 365

- Windows Server 2008 — wersje Standard, Enterprise, Datacenter, Foundation i Web (tylko x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter, Foundation i Web
- Windows Home Server 2011
- Windows Small Business Server 2011 — wszystkie wersje
- Windows 8/8.1 — wszystkie wersje (tylko 64-bitowe) oprócz Windows RT
- Windows Server 2012/2012 R2 — wszystkie wersje

© Acronis International GmbH, 2003-2024

- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (tylko x64)
- Windows 10 — wersje Home, Pro, Education i Enterprise (tylko x64)
- Windows Server 2016 — wszystkie opcje instalacji (tylko x64) z wyjątkiem serwera Nano Server
- Windows Server 2019 — wszystkie opcje instalacji (tylko x64) z wyjątkiem serwera Nano Server
- Windows 11 — wszystkie wersje
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Agent dla programu Oracle

- Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter i Web (x86, x64)
- Windows Server 2012 R2 — wersje Standard, Enterprise, Datacenter i Web (x86, x64)
- Linux — dowolne jądro i dowolna dystrybucja obsługiwane przez agenta dla systemu Linux (wymieniono niżej)

Agent dla MySQL/MariaDB

- Linux — dowolne jądro i dowolna dystrybucja obsługiwane przez agenta dla systemu Linux (wymieniono niżej)

Agent dla systemu Linux

Ten agent obejmuje komponent na potrzeby usług Ochrona przed wirusami i złośliwym oprogramowaniem oraz Filtrowanie adresów URL. Szczegółowe informacje na temat funkcji obsługiwanych w systemach operacyjnych można znaleźć w sekcji "Obsługa funkcji ochrony w poszczególnych systemach operacyjnych" (s. 47).

Poniższe dystrybucje i wersje jądra systemu Linux zostały specjalnie przetestowane. Ale nawet jeśli dana dystrybucja lub wersja jądra systemu Linux nie jest niżej wymieniona, to ze względu na specyfikę systemów operacyjnych Linux może wciąż poprawnie działać we wszystkich wymaganych zastosowaniach.

Jeśli w przypadku korzystania z programu Cyber Protection w połączeniu z daną dystrybucją i wersją jądra systemu Linux wystąpią problemy, skontaktuj się z zespołem pomocy technicznej w celu przeprowadzenia dokładniejszego dochodzenia.

Linux z jądrem w wersjach od 2.6.9 do 5.19 i biblioteką glibc w wersji 2.3.4 lub nowszą, w tym następujące dystrybucje x86 i x86_64:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15

© Acronis International GmbH, 2003-2024

Ważne
W przypadku systemów SUSE Linux Enterprise Server 12 i SUSE Linux Enterprise Server 15 nie są obsługiwane konfiguracje z systemem plików Btrfs.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3* — wersje Unbreakable Enterprise Kernel i Red Hat Compatible Kernel

Uwaga
Instalacja agenta ochrony w systemie Oracle Linux 8.6 lub nowszym z włączoną funkcją Secure Boot wymaga ręcznego podpisania modułów jądra. Dodatkowe informacje na temat podpisywania modułu jądra można znaleźć w tym artykule z bazy wiedzy Knowledge Base.

- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* Od wersji 8.4 obsługa jest dostępna tylko w przypadku jąder w wersji od 4.18 do 5.19

Agent dla systemu Mac

Ten agent obejmuje komponent na potrzeby usług Ochrona przed wirusami i złośliwym oprogramowaniem oraz Filtrowanie adresów URL. Szczegółowe informacje na temat funkcji obsługiwanych w systemach operacyjnych można znaleźć w sekcji "Obsługa funkcji ochrony w poszczególnych systemach operacyjnych" (s. 47).

Obsługiwana jest zarówno architektura x64, jak i ARM (stosowana w procesorach Apple Silicon, takich jak Apple M1 i M2).

Uwaga
Nie można odzyskać kopii zapasowych na poziomie dysku z komputerów Mac z procesorami Intel na komputery Mac z procesorami Apple Silicon i na odwrót. Można odzyskać pliki i foldery.

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11

© Acronis International GmbH, 2003-2024

- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

Ważne
Od wersji C23.07 platforma Cyber Protect Cloud nie obsługuje następujących systemów operacyjnych: OS X Yosemite 10.10, OS X El Capitan 10.11 i macOS Sierra 10.12.

Zdecydowanie zalecamy zaktualizowanie systemu operacyjnego do obsługiwanej wersji w celu zapewnienia kompatybilności i zyskania możliwości korzystania ze wszystkich funkcji platformy Cyber Protect Cloud.

Agent dla VMware (urządzenie wirtualne)

Ten agent jest udostępniany jako urządzenie wirtualne do uruchomienia na hoście ESXi.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Agent dla VMware (Windows)

Ten agent jest udostępniany jako aplikacja systemu Windows do uruchomienia w dowolnym z systemów operacyjnych wymienionych powyżej w obszarze Agent dla systemu Windows z następującymi wyjątkami:

- 32-bitowe systemy operacyjne nie są obsługiwane.
- Systemy Windows XP, Windows Server 2003/2003 R2 i Windows Small Business Server 2003/2003 R2 nie są obsługiwane.

Agent dla Hyper-V

- Windows Server 2008 (tylko x64) z rolą Hyper-V, w tym tryb instalacji Server Core
- Windows Server 2008 R2 z rolą Hyper-V, w tym tryb instalacji Server Core
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 z rolą Hyper-V, w tym tryb instalacji Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (tylko x64) z rolą Hyper-V
- Windows 10 — wersje Pro, Education i Enterprise z rolą Hyper-V
- Windows Server 2016 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

© Acronis International GmbH, 2003-2024

- Microsoft Hyper-V Server 2019
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Agent dla Virtuozzo

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

Agent dla Virtuozzo Hybrid Infrastructure

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0

Agent dla Scale Computing HC3

Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3

Agent dla oVirt

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agent dla Synology

DiskStation Manager 6.2.x, 7.x

Agent dla Synology obsługuje tylko urządzenia NAS z procesorami x86_64. Procesory ARM nie są obsługiwane.

Cyber Protect Monitor

- Windows 7 lub nowszy
- Windows Server 2008 R2 lub nowszy
- Wszystkie wersje systemu macOS obsługiwane przez agenta dla systemu Mac

Obsługiwane wersje programu Microsoft SQL Server

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2

© Acronis International GmbH, 2003-2024

- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

Obsługiwane są też wersje oprogramowania SQL Server Express wyżej wymienionych wersji SQL Server.

Uwaga
Kopie zapasowe Microsoft SQL są obsługiwane tylko w przypadku baz danych działających w systemach plików NFTS, REFS i FAT32. System plików ExFat nie jest obsługiwany.

Obsługiwane wersje programu Microsoft Exchange Server

- Microsoft Exchange Server 2019 — wszystkie wersje.
- Microsoft Exchange Server 2016 — wszystkie wersje.
- Microsoft Exchange Server 2013 — wszystkie wersje, aktualizacja Cumulative Update 1 (CU1) i nowsze.
- Microsoft Exchange Server 2010 — wszystkie wersje, wszystkie dodatki Service Pack. Kopie zapasowe skrzynki pocztowej i odzyskiwanie granularne z kopii zapasowej bazy danych są obsługiwane od wersji z dodatkiem Service Pack 1 (SP1).
- Microsoft Exchange Server 2007 — wszystkie wersje, wszystkie dodatki Service Pack. Kopie zapasowe skrzynki pocztowej i odzyskiwanie granularne z kopii zapasowej bazy danych nie są obsługiwane.

Obsługiwane wersje programu Microsoft SharePoint

Program Cyber Protection obsługuje następujące wersje programu Microsoft SharePoint:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*Aby można było używać narzędzia SharePoint Explorer z tymi wersjami, musi być dostępna farma odzyskiwania programu SharePoint, do której będzie można dołączyć bazy danych.

Kopie zapasowe lub bazy danych, z których są wyodrębniane dane, muszą pochodzić z tej samej wersji programu SharePoint co wersja, w której jest zainstalowane narzędzie SharePoint Explorer.

Obsługiwane wersje systemu Oracle Database

- Oracle Database w wersji 11g, wszystkie wydania
- Oracle Database w wersji 12c, wszystkie wydania

© Acronis International GmbH, 2003-2024

- Oracle Database w wersji 19c, wszystkie wydania
- Oracle Database w wersji 21c, wszystkie wydania

Obsługiwane są tylko konfiguracje obejmujące jedną instancję.

Obsługiwane wersje platformy SAP HANA

Platforma HANA 2.0 SPS 03 zainstalowana w systemie RHEL 7.6 działającym na komputerze fizycznym lub maszynie wirtualnej VMware ESXi.

Ponieważ platforma SAP HANA nie obsługuje odzyskiwania kontenerów baz danych z wieloma dzierżawcami przy użyciu migawek pamięci masowej, rozwiązanie to obsługuje kontenery SAP HANA z bazy danych z tylko jednym dzierżawcą.

Obsługiwane wersje programu MySQL

- 5.5.x — wersje Community Server, Enterprise, Standard i Classic
- 5.6.x — wersje Community Server, Enterprise, Standard i Classic
- 5.7.x — wersje Community Server, Enterprise, Standard i Classic
- 8.0.x — wersje Community Server, Enterprise, Standard i Classic

Obsługiwane wersje systemu MariaDB

- 10.0.x
- 10.1.x
- 10.2.x
- 10.3.x
- 10.4.x
- 10.5.x
- 10.6.x
- 10.7.x

Obsługiwane platformy wirtualizacji

W poniższej tabeli zestawiono możliwości obsługi poszczególnych platform wirtualizacji.

Więcej informacji na temat różnic między operacjami tworzenia kopii zapasowych za pomocą agenta a operacjami tworzenia kopii zapasowych bezagentowo można znaleźć w sekcji "Tworzenie kopii zapasowych przy użyciu agenta i bezagentowe" (s. 66).

© Acronis International GmbH, 2003-2024

Uwaga
Jeśli korzystasz z platformy wirtualizacji lub jej wersji, która nie jest wymieniona poniżej, metoda **Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)** powinna nadal działać poprawnie we wszystkich wymaganych scenariuszach. Jeśli napotkasz problemy z utworzeniem kopii zapasowej przy użyciu agenta, skontaktuj się z zespołem pomocy technicznej w celu ich dokładniejszego zbadania.

VMware

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Wersje środowiska VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **Wersje środowiska VMware vSphere:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **VMware ESXi** > **Agent do zainstalowania w systemie Windows** lub **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **VMware ESXi** > **Urządzenie wirtualne (OVF)**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
VMware vSphere Hypervisor (Free ESXi)**	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
VMware Server (serwer VMware Virtual) VMware Workstation VMware ACE VMware Player	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

* W tych edycjach transport HotAdd w przypadku dysków wirtualnych jest obsługiwany przez środowisko vSphere w wersji 5.0 lub nowszej. W wersji 4.1 operacje tworzenia kopii zapasowych mogą być wolniej realizowane.

© Acronis International GmbH, 2003-2024

** Tworzenie kopii zapasowych na poziomie hiperwizora nie jest obsługiwane w przypadku programu vSphere Hypervisor, ponieważ ogranicza on dostęp do interfejsu Remote Command Line Interface (RCLI) do trybu tylko do odczytu. Agent działa w trakcie okresu próbnego programu vSphere Hypervisor przed wprowadzeniem klucza seryjnego. Po wprowadzeniu klucza seryjnego agent przestaje działać.

Uwaga
Cyber Protect Cloud oficjalnie obsługuje każdą aktualizację dostępną w ramach obsługiwanej wersji głównej środowiska vSphere.

Na przykład obsługa vSphere 8.0 obejmuje obsługę każdej aktualizacji w ramach tej wersji, chyba że określono inaczej. A zatem obsługa pierwotnie wydanego vSphere 8.0 oznacza też obsługę vSphere 8.0 Update 1.

Obsługa określonej wersji środowiska VMware vSphere oznacza, że obsługiwane jest również oprogramowanie vSAN w tej analogicznej wersji. Na przykład obsługa środowiska vSphere 8.0 oznacza, że obsługiwane jest również oprogramowanie vSAN 8.0.

Ograniczenia

- **Komputery odporne na awarie**
  Agent dla VMware tworzy kopię zapasową komputera odpornego na awarie tylko wtedy, gdy w środowisku VMware vSphere w wersji 6.0 lub nowszej została włączona odporność na awarie. Jeśli środowisko vSphere zostało uaktualnione ze starszej wersji, wystarczy na każdym komputerze wyłączyć i włączyć odporność na awarie. Jeśli korzystasz ze starszej wersji środowiska vSphere, zainstaluj agenta systemie operacyjnym-gościu.
- **Dyski niezależne i RDM**
  Agent dla VMware nie tworzy kopii zapasowych dysków Raw Device Mapping (RDM) w trybie kompatybilności fizycznej ani dysków niezależnych. Agent pomija te dyski i dodaje ostrzeżenia do dziennika. Ostrzeżeń tych można uniknąć, wykluczając dyski niezależne i RDM w trybie kompatybilności fizycznej z planu ochrony. Aby utworzyć kopię zapasową tych dysków lub znajdujących się na nich danych, zainstaluj agenta w systemie operacyjnym-gościu.
- **Połączenie iSCSI w systemie-gościu**
  Agent dla VMware nie tworzy kopii zapasowych woluminów LUN podłączonych przez inicjator iSCSI działający w systemie operacyjnym gościa. Ponieważ hiperwizor ESXi nie rozpoznaje takich woluminów, woluminy te nie są uwzględniane w migawkach na poziomie hiperwizora i są bez ostrzeżenia pomijane podczas tworzenia kopii zapasowej. Aby utworzyć kopię zapasową takich woluminów lub znajdujących się na nich danych, należy zainstalować agenta w systemie operacyjnym-gościu.
- **Szyfrowane maszyny wirtualne** (wprowadzone w środowisku VMware vSphere 6.5)
  - Szyfrowane maszyny wirtualne są zapisywane w kopii zapasowej w stanie niezaszyfrowanym. Jeśli szyfrowanie ma znaczenie krytyczne, włącz szyfrowanie kopii zapasowych podczas tworzenia planu ochrony.
  - Odzyskane maszyny wirtualne nigdy nie są zaszyfrowane. Po zakończeniu odzyskiwania można szyfrowanie włączyć ręcznie.

© Acronis International GmbH, 2003-2024

- Jeśli tworzysz kopie zapasowe szyfrowanych maszyn wirtualnych, zalecamy zaszyfrowanie również maszyny, na której działa agent dla VMware. W przeciwnym razie tempo operacji dotyczących szyfrowanych maszyn może być poniżej oczekiwań. Zastosuj **Zasady szyfrowania maszyn wirtualnych** do maszyny agenta przy użyciu klienta internetowego vSphere.
- Kopie zapasowe szyfrowanych maszyn wirtualnych zostaną utworzone przy użyciu sieci lokalnej nawet w przypadku skonfigurowania dla agenta trybu transportu SAN. Ponieważ środowisko VMware nie obsługuje tworzenia kopii zapasowych zaszyfrowanych dysków wirtualnych w trybie transportu SAN, agent wykona przełączenie awaryjne na tryb transportu NBD.

- **Secure Boot**
  - Maszyny wirtualne VMware: po odzyskaniu maszyny wirtualnej jako nowej maszyny funkcja **Secure Boot** (wprowadzona w środowisku VMware vSphere 6.5) jest wyłączona. Po zakończeniu odzyskiwania można tę opcję włączyć ręcznie. To ograniczenie dotyczy technologii VMware.
  - Maszyny wirtualne Hyper-V: w przypadku wszystkich maszyn wirtualnych generacji 2 funkcja Secure Boot jest wyłączana po odzyskaniu komputera zarówno na nową, jak i na już istniejącą maszynę wirtualną.
- **Kopie zapasowe konfiguracji ESXi** nie są obsługiwane w przypadku środowiska VMware vSphere w wersji 7.0 lub nowszej.
- **Maszyny wirtualne z pustym identyfikatorem UUID instancji nie są widoczne w konsoli Cyber Protect**

  Maszyny wirtualne VMware z pustą właściwością vSphere `UUID instancji` (`vc.uuid`) nie są widoczne na liście w konsoli Cyber Protect. Więcej informacji na temat rozwiązywania tego problemu można znaleźć w tym artykule bazy wiedzy Knowledge Base.
- **Ustawienia sieciowe agenta ochrony**

  Utworzenie kopii zapasowej maszyny wirtualnej VMware może się nie powieść, jeśli agent ochrony nie będzie w stanie rozpoznać nazwy hosta ESXi zarejestrowanej w vCenter jako powiązanej z adresem IP, nawet jeśli może rozpoznać nazwę hosta vCenter. Wyświetlany jest następujący błąd: „Nie masz praw dostępu do tego pliku”.

  Aby rozwiązać ten problem, edytuj ustawienia sieciowe agenta ochrony, konfigurując usługę DNS lub modyfikując plik `/etc/hosts`. Aby sprawdzić poprawkę, na komputerze z agentem ochrony uruchom następujące polecenie:

  ```
  ping <ESXi host name>
  ```
- **Operacje obsługiwane na komputerach z woluminami logicznymi**

  Tworzenie kopii zapasowych i odzyskiwanie maszyn z woluminami logicznymi, takimi jak LDM w systemie Windows (dyski dynamiczne) czy LVM w systemie Linux, jest obsługiwane z pewnymi ograniczeniami. Więcej informacji na temat ograniczeń można znaleźć w sekcji "Obsługiwane operacje na woluminach logicznych" (s. 61).

© Acronis International GmbH, 2003-2024

Microsoft

Hyper-V maszyny wirtualne działające w hiperkonwergentnym klastrze z Storage Spaces Direct (S2D) są obsługiwane. Storage Spaces Direct jest też obsługiwane jako magazyn kopii zapasowych.

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Windows Server 2008 (x64) z serwerem Hyper-V Windows Server 2008 R2 z rolą Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 z rolą Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) z technologią Hyper-V Windows 10 z technologią Hyper-V Windows Server 2016 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Hyper-V**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje**

© Acronis International GmbH, 2003-2024

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
		robocze albo **Serwery** > **Windows** lub **Linux**
Microsoft Virtual Server 2005	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

Uwaga
Obsługiwane są maszyny wirtualne Hyper-V działające w klastrze hiperkonwergentnym z rozwiązaniem Storage Spaces Direct (S2D). Rozwiązanie Storage Spaces Direct jest też obsługiwane jako magazyn kopii zapasowych.

Ograniczenia

- **Dyski pass-through**
  Agent dla Hyper-V nie tworzy kopii zapasowych dysków pass-through. Podczas tworzenia kopii zapasowej agent pomija te dyski i dodaje ostrzeżenia do dziennika. Ostrzeżeń tych można uniknąć, wykluczając dyski pass-through z planu ochrony. Aby utworzyć kopię zapasową tych dysków lub znajdujących się na nich danych, zainstaluj agenta w systemie operacyjnym-gościu.
- **Klastrowanie gości Hyper-V**
  Agent dla Hyper-V nie obsługuje tworzenia kopii zapasowych maszyn wirtualnych Hyper-V będących węzłami klastra awaryjnego systemu Windows Server. Migawka VSS na poziomie hosta może nawet tymczasowo odłączyć zewnętrzny dysk kworum od klastra. Aby utworzyć kopię zapasową tych maszyn, zainstaluj agenty w systemach operacyjnych-gościach.
- **Połączenie iSCSI w systemie-gościu**
  Agent dla Hyper-V nie tworzy kopii zapasowych woluminów LUN podłączonych przez inicjator iSCSI działający w systemie operacyjnym gościa. Ponieważ hiperwizor Hyper-V nie rozpoznaje takich woluminów, woluminy te nie są uwzględniane w migawkach na poziomie hiperwizora i są bez ostrzeżenia pomijane podczas tworzenia kopii zapasowej. Aby utworzyć kopię zapasową takich woluminów lub znajdujących się na nich danych, należy zainstalować agenta w systemie operacyjnym-gościu.
- **Nazwy plików VHD/VHDX z symbolem &**
  Na hostach Hyper-V z systemem Windows Server 2016 lub nowszym nie można tworzyć kopii zapasowych starszych maszyn wirtualnych (wersja 5.0) utworzonych pierwotnie przy użyciu oprogramowania Hyper-V 2012 R2 lub starszego, jeśli nazwy ich plików VHD/VHDX zawierają symbol &.

© Acronis International GmbH, 2003-2024

Aby móc utworzyć kopię zapasową takich maszyn, należy w Menedżerze Hyper-V odłączyć odpowiedni dysk wirtualny od maszyny wirtualnej, edytować nazwę pliku VHD/VHDX tak, aby usunąć symbol &, a następnie podłączyć dysk z powrotem do maszyny wirtualnej.

- **Zależność od podsystemu Microsoft WMI**

  Bezagentowe tworzenie kopii zapasowych maszyn wirtualnych Hyper-V zależy od podsystemu Microsoft WMI, a w szczególności od klasy `Msvm_VirtualSystemManagementService`. Jeśli zapytania WMI się nie powiodą, tworzenie kopii zapasowych również się nie powiedzie. Więcej informacji na temat klasy `Msvm_VirtualSystemManagementService` można znaleźć w dokumentacji firmy Microsoft.
- **Maszyny wirtualne z dyskami PMEM**

  Tworzenie kopii zapasowych maszyn wirtualnych Hyper-V z dyskami z pamięcią trwałą (PMEM) nie jest obsługiwane.
- **Odzyskiwanie na inną platformę**

  Jeśli agent dla Hyper-V odzyska kopię zapasową utworzoną przez innego agenta jako nową maszynę wirtualną Hyper-V, powstała maszyna będzie maszyną pierwszej generacji.
- **Secure Boot**

  W celu zagwarantowania możliwości uruchomienia maszyn wirtualnych Hyper-V drugiej generacji, które odzyskano, funkcja Secure Boot zostaje wyłączona. Możesz ponownie włączyć tę funkcję ręcznie w narzędziu do zarządzania Hyper-V. Więcej informacji na temat funkcji Secure Boot i maszyn wirtualnych drugiej generacji można znaleźć w dokumentacji firmy Microsoft.
- **Kopie zapasowe maszyn wirtualnych z systemem Linux spójne ze stanem awarii**

  Kopie zapasowe maszyn wirtualnych z systemem Linux działających na hoście z funkcją Hyper-V 2019 są przełączane awaryjnie na migawki spójne ze stanem awarii ze względu na ograniczenia rozwiązania firmy Microsoft (brak możliwości utworzenia punktów kontrolnych w środowisku produkcyjnym dla maszyn wirtualnych z systemem Linux). Aby uniknąć ostrzeżeń podczas tworzenia kopii zapasowej, wyłącz opcję tworzenia kopii zapasowych Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych w planie ochrony.
- **Uruchamianie maszyny wirtualnej z kopii zapasowej**

  Uruchomienie maszyny wirtualnej z kopii zapasowej na hoście Hyper-V się nie powiedzie, jeśli kopia zapasowa znajduje się na tym samym woluminie co ścieżka wybrana dla zamontowanych dysków maszyny wirtualnej. Aby rozwiązać ten problem, wybierz inny wolumin jako ścieżkę zamontowanych dysków maszyny wirtualnej. Przestrzeń ta będzie wykorzystywana wyłącznie na zmiany generowane w ramach zamontowanej maszyny wirtualnej i nie zajmie całego rozmiaru dysku wirtualnego.
- **Operacje obsługiwane na komputerach z woluminami logicznymi**

  Tworzenie kopii zapasowych i odzyskiwanie maszyn z woluminami logicznymi, takimi jak LDM w systemie Windows (dyski dynamiczne) czy LVM w systemie Linux, jest obsługiwane z pewnymi ograniczeniami. Więcej informacji na temat ograniczeń można znaleźć w sekcji "Obsługiwane operacje na woluminach logicznych" (s. 61).

© Acronis International GmbH, 2003-2024

Scale Computing

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Scale Computing HC3**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

Ograniczenia

Operacje obsługiwane na komputerach z woluminami logicznymi

Tworzenie kopii zapasowych i odzyskiwanie maszyn z woluminami logicznymi, takimi jak LDM w systemie Windows (dyski dynamiczne) czy LVM w systemie Linux, jest obsługiwane z pewnymi ograniczeniami. Więcej informacji na temat ograniczeń można znaleźć w sekcji "Obsługiwane operacje na woluminach logicznych" (s. 61).

Citrix

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Citrix XenServer/Citrix Hypervisor 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2	Nieobsługiwana	Obsługiwane tylko w przypadku gości w pełni zwirtualizowanych (znanych jako HVM). Parawirtualne maszyny-goście (PV) nie są obsługiwane. **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Citrix XenServer** > **Windows** lub **Linux**

© Acronis International GmbH, 2003-2024

Red Hat i Linux

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Red Hat Virtualization (zarządzany przez oVirt) 4.2, 4.3, 4.4, 4.5	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Red Hat Virtualization (oVirt)**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Maszyny wirtualne oparte na jądrze (KVM)	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **KVM** > **Windows** lub **Linux**
Maszyny wirtualne oparte na jądrze (KVM) zarządzane przez oVirt 4.3 działający w systemie Red Hat Enterprise Linux 7.6 bądź 7.7 lub CentOS 7.6 bądź 7.7	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Red Hat Virtualization (oVirt)**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Maszyny wirtualne oparte na jądrze (KVM) zarządzane przez oVirt 4.4 działający w systemie Red Hat Enterprise Linux 8.x lub CentOS Stream 8.x	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Red Hat Virtualization (oVirt)**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Maszyny wirtualne oparte na jądrze (KVM) zarządzane przez oVirt 4.5 działający w systemie Red Hat Enterprise Linux 8.x lub CentOS Stream 8.x	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Red Hat Virtualization (oVirt)**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

Ograniczenia

Operacje obsługiwane na komputerach z woluminami logicznymi

Tworzenie kopii zapasowych i odzyskiwanie maszyn z woluminami logicznymi, takimi jak LDM w systemie Windows (dyski dynamiczne) czy LVM w systemie Linux, jest obsługiwane z pewnymi

© Acronis International GmbH, 2003-2024

ograniczeniami. Więcej informacji na temat ograniczeń można znaleźć w sekcji "Obsługiwane operacje na woluminach logicznych" (s. 61).

Parallels

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Parallels Workstation	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Parallels Server 4 Bare Metal	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

Oracle

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Oracle Virtualization Manager (oparty na środowisku oVirt)* 4.3	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Red Hat Virtualization (oVirt)**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Oracle VM Server 3.0, 3.3, 3.4	Nieobsługiwana	Obsługiwane tylko w przypadku gości w pełni zwirtualizowanych (znanych jako HVM). Parawirtualne maszyny-goście (PV) nie są obsługiwane. **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Oracle** > **Windows** lub **Linux**
Oracle VM VirtualBox 4.x	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Oracle** > **Windows** lub **Linux**

© Acronis International GmbH, 2003-2024

* Oracle Virtualization Manager jest obsługiwany tylko przez agenta dla oVirt.

Ograniczenia

Operacje obsługiwane na komputerach z woluminami logicznymi

Tworzenie kopii zapasowych i odzyskiwanie maszyn z woluminami logicznymi, takimi jak LDM w systemie Windows (dyski dynamiczne) czy LVM w systemie Linux, jest obsługiwane z pewnymi ograniczeniami. Więcej informacji na temat ograniczeń można znaleźć w sekcji "Obsługiwane operacje na woluminach logicznych" (s. 61).

Nutanix

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Hiperwizor Nutanix Acropolis (AHV) w wersji od 20160925.x do 20180425.x	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Nutanix AHV** > **Windows** lub **Linux**

Virtuozzo

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Virtuozzo**	Obsługiwane tylko w przypadku maszyn wirtualnych. Kontenery nie są obsługiwane. **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Virtuozzo 7.0.13, 7.0.14	Obsługiwane tylko w przypadku kontenerów ploop. Maszyny wirtualne nie są obsługiwane. **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Virtuozzo**	Obsługiwane tylko w przypadku maszyn wirtualnych. Kontenery nie są obsługiwane. **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**
Virtuozzo Hybrid Server 7.5	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty**	Obsługiwane tylko w przypadku maszyn wirtualnych. Kontenery

© Acronis International GmbH, 2003-2024

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
	wirtualizacji > **Virtuozzo**	nie są obsługiwane. **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

Ograniczenia

Operacje obsługiwane na komputerach z woluminami logicznymi

Tworzenie kopii zapasowych i odzyskiwanie maszyn z woluminami logicznymi, takimi jak LDM w systemie Windows (dyski dynamiczne) czy LVM w systemie Linux, jest obsługiwane z pewnymi ograniczeniami. Więcej informacji na temat ograniczeń można znaleźć w sekcji "Obsługiwane operacje na woluminach logicznych" (s. 61).

Virtuozzo Hybrid Infrastructure

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	Obsługiwane **Urządzenia** > **Dodaj** > **Hosty wirtualizacji** > **Virtuozzo Hybrid Infrastructure**	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

Ograniczenia

- **Bezagentowe tworzenie kopii zapasowych maszyn wirtualnych przy użyciu dysków w zewnętrznej pamięci masowej iSCSI**
  Nie można tworzyć kopii zapasowych maszyn wirtualnych z poziomu Virtuozzo Hybrid Infrastructure, jeśli dyski maszyn wirtualnych znajdują się na zewnętrznych woluminach iSCSI (podłączonych do klastra VHI).
- **Operacje obsługiwane na komputerach z woluminami logicznymi**
  Tworzenie kopii zapasowych i odzyskiwanie maszyn z woluminami logicznymi, takimi jak LDM w systemie Windows (dyski dynamiczne) czy LVM w systemie Linux, jest obsługiwane z pewnymi ograniczeniami. Więcej informacji na temat ograniczeń można znaleźć w sekcji "Obsługiwane operacje na woluminach logicznych" (s. 61).

© Acronis International GmbH, 2003-2024

Amazon

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Instancje środowiska Amazon EC2	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

Microsoft Azure

Platforma	Bezagentowe tworzenie kopii zapasowych (na poziomie hiperwizora)	Tworzenie kopii zapasowych przy użyciu agenta (z systemu operacyjnego gościa)
Maszyny wirtualne Azure	Nieobsługiwana	Obsługiwane **Urządzenia** > **Dodaj** > **Stacje robocze** albo **Serwery** > **Windows** lub **Linux**

Kompatybilność z programami szyfrującymi

W przypadku tworzenia kopii zapasowych i odzyskiwania danych szyfrowanych za pomocą oprogramowania szyfrującego *na poziomie plików* nie występują żadne ograniczenia.

Oprogramowanie szyfrujące *na poziomie dysku* szyfruje dane w locie. Dlatego dane w kopii zapasowej są w postaci niezaszyfrowanej. Programy szyfrujące na poziomie dysku często modyfikują obszary systemowe: rekordy rozruchowe, tabele partycji lub tabele systemów plików. Te czynniki wpływają na tworzenie kopii zapasowych na poziomie dysku i odzyskiwanie z nich danych, a także możliwości uruchamiania odzyskanego systemu i dostępu do strefy Secure Zone.

Można tworzyć kopie zapasowe danych zaszyfrowanych przy użyciu następujących programów szyfrujących na poziomie dysku:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

Aby zapewnić niezawodne odzyskiwanie na poziomie dysku, postępuj zgodnie z powszechnymi regułami oraz zaleceniami dotyczącymi konkretnych programów.

© Acronis International GmbH, 2003-2024

Powszechna reguła dotycząca instalacji

Zdecydowanie zalecamy zainstalowanie oprogramowania szyfrującego przed rozpoczęciem instalacji agentów ochrony.

Sposób korzystania ze strefy Secure Zone

Strefa Secure Zone nie może być zaszyfrowana na poziomie dysku. Ze strefy Secure Zone można korzystać tylko następująco:

1. Zainstaluj oprogramowanie szyfrujące, a następnie zainstaluj agenta.
2. Utwórz strefę Secure Zone.
3. Wyklucz strefę Secure Zone podczas szyfrowania dysku lub jego woluminów.

Powszechna reguła dotycząca tworzenia kopii zapasowych

Kopię zapasową na poziomie dysku można utworzyć pod kontrolą systemu operacyjnego.

Procedury odzyskiwania dotyczące konkretnych programów

Microsoft BitLocker Drive Encryption

Aby odzyskać system zaszyfrowany przez program BitLocker:

1. Uruchom komputer za pomocą nośnika startowego.
2. Odzyskaj system. Odzyskane dane będą w postaci niezaszyfrowanej.
3. Ponownie uruchom odzyskany system.
4. Włącz program BitLocker.

Jeśli musisz odzyskać tylko jedną z wielu partycji dysku, wykonaj tę operację pod kontrolą systemu operacyjnego. Odzyskiwanie za pomocą nośnika startowego może spowodować, że odzyskana partycja nie będzie wykrywana w systemie Windows.

McAfee Endpoint Encryption i PGP Whole Disk Encryption

Zaszyfrowaną partycję systemową można odzyskać tylko przy użyciu nośnika startowego.

Jeśli odzyskany system się nie uruchomi, odbuduj główny rekord startowy zgodnie z opisem podanym w artykule bazy wiedzy Microsoft Knowledge Base: https://support.microsoft.com/kb/2622803.

Kompatybilność z urządzeniami pamięci masowej Dell EMC Data Domain

Można używać urządzeń Dell EMC Data Domain jako magazynów kopii zapasowych.

© Acronis International GmbH, 2003-2024

W przypadku tego magazynu zalecamy korzystanie ze schematu tworzenia kopii zapasowych, który regularnie tworzy pełne kopie zapasowe, na przykład **Zawsze pełna**. Aby dowiedzieć się więcej o dostępnych schematach tworzenia kopii zapasowych, zobacz "Schematy tworzenia kopii zapasowych" (s. 447).

Blokada przechowywania

Obsługiwana jest blokada przechowywania (tryb nadzoru). Jeśli w magazynie Data Domain jest włączona blokada przechowywania, trzeba dodać zmienną środowiskową `AR_RETENTION_LOCK_SUPPORT` do komputera z agentem ochrony, który używa tego magazynu jako lokalizacji docelowej kopii zapasowych. Aby uzyskać więcej informacji, zobacz sekcję "Dodawanie zmiennej AR_RETENTION_LOCK_SUPPORT" (s. 46).

Uwaga
Urządzenia pamięci masowej Dell EMC Data Domain z włączoną blokadą przechowywania nie są obsługiwane przez agenta dla systemu Mac.

Jeśli w magazynie Data Domain jest włączona blokada przechowywania, kopie zapasowe przechowywane w tym magazynie nie zostaną usunięte zgodnie z regułami przechowywania zdefiniowanymi w planie ochrony. Żaden błąd nie zostanie wyświetlony. Kopie zapasowe zostaną usunięte po wygaśnięciu blokady przechowywania, a wówczas reguły przechowywania zostaną ponownie zastosowane.

W zależności od konfiguracji planu ochrony reguły przechowywania są stosowane do archiwum przed utworzeniem kopii zapasowej lub po jej utworzeniu.

Dodawanie zmiennej AR_RETENTION_LOCK_SUPPORT

Jeśli w magazynie Data Domain jest włączona blokada przechowywania, trzeba dodać zmienną środowiskową `AR_RETENTION_LOCK_SUPPORT` do komputera z agentem ochrony, który używa tego magazynu jako lokalizacji docelowej kopii zapasowych.

Aby dodać zmienną środowiskową `AR_RETENTION_LOCK_SUPPORT`

W systemie Windows

1. Zaloguj się jako administrator na komputerze lub maszynie wirtualnej z agentem ochrony.
2. W oknie **Panel sterowania** wybierz kolejno **System i zabezpieczenia** > **System** > **Zaawansowane zabezpieczenia systemu**.
3. Na karcie **Zaawansowane** kliknij **Zmienne środowiskowe**.
4. W panelu **Zmienne systemowe** kliknij **Nowa**.
5. W oknie **Nowa zmienna systemowa** dodaj następującą nową zmienną:
   - Nazwa zmiennej: `AR_RETENTION_LOCK_SUPPORT`
   - Wartość zmiennej: `1`
6. Kliknij **OK**.

© Acronis International GmbH, 2003-2024

7. W oknie **Zmienne środowiskowe** kliknij **OK**.
8. Uruchom ponownie komputer.

W systemie Linux

1. Zaloguj się jako administrator na komputerze lub maszynie wirtualnej z agentem ochrony.
2. Przejdź do katalogu `/sbin`, a następnie otwórz plik `acronis_mms` do edycji.
3. Na wierszem `export LD_LIBRARY_PATH` dodaj następujący wiersz:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Zapisz plik `acronis_mms`.
5. Uruchom ponownie komputer.

Na urządzeniu wirtualnym

1. Zaloguj się na urządzeniu wirtualnym jako administrator.
2. Przejdź do katalogu `/bin`, a następnie otwórz plik `autostart` do edycji.
3. Pod wierszem `export LD_LIBRARY_PATH` dodaj następujący wiersz:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Zapisz plik `autostart`.
5. Uruchom ponownie urządzenie wirtualne.

Obsługa funkcji ochrony w poszczególnych systemach operacyjnych

Ten temat zawiera informacje o funkcjach ochrony platformy Cyber Protect Cloud. Nie ma tu listy funkcji tworzenia kopii zapasowych i odzyskiwania.

Funkcje ochrony są obsługiwane tylko w przypadku komputerów z zainstalowanym agentem ochrony. Nie są dostępne w przypadku maszyn wirtualnych, których kopie zapasowe są tworzone w trybie bezagentowym, np. przez agenta dla Hyper-V, agenta dla VMware, agenta dla Virtuozzo Hybrid Infrastructure, agenta dla Scale Computing lub agenta dla oVirt.

Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Obsługiwane systemy operacyjne i wersje

Windows

Jeśli nie określono inaczej w kontekście danego zestawu funkcji, obsługiwane są następujące wersje systemu Windows:

© Acronis International GmbH, 2003-2024

- Windows 7 Service Pack 1 lub nowszy
- Windows Server 2008 R2 Service Pack 1 i nowsze

Uwaga
W przypadku systemu Windows 7 przed zainstalowaniem agenta ochrony trzeba zainstalować poniższe aktualizacje od firmy Microsoft.

- Rozszerzone aktualizacje zabezpieczeń (ESU) systemu Windows 7
- KB4474419
- KB4490628

Więcej informacji na temat wymaganych aktualizacji można znaleźć w tym artykule bazy wiedzy Knowledge Base.

Linux

Obsługiwane dystrybucje systemu Linux i ich wersje zależą od zestawów funkcji i są widoczne u dołu każdej tabeli.

macOS

Obsługiwane wersje systemu macOS zależą od zestawów funkcji i są widoczne u dołu każdej tabeli.

Zestaw funkcji	Windows	Linux	macOS
Domyślne plany ochrony			
Pracownicy zdalni	Tak	Nie	Nie
Pracownicy w biurze (program antywirusowy innej firmy)	Tak	Nie	Nie
Pracownicy w biurze (ochrona antywirusowa Cyber Protect)	Tak	Nie	Nie
Cyber Protect Essentials (tylko w przypadku wersji Cyber Protect Essentials)	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Kopia zapasowa na potrzeby analizy śledczej			
Zapisanie surowego zrzutu pamięci	Tak	Nie	Nie
Migawka uruchomionych procesów	Tak	Nie	Nie
Notaryzacja lokalnej kopii zapasowej obrazu na potrzeby analizy śledczej	Tak	Nie	Nie

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Kopia zapasowa na potrzeby analizy śledczej			
Notaryzacja chmurowej kopii zapasowej obrazu na potrzeby analizy śledczej	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Funkcje	Windows	Linux	macOS
Ciągła ochrona danych			
Ciągła ochrona plików i folderów	Tak	Nie	Nie
Ciągła ochrona zmienianych plików przy użyciu funkcji śledzenia aplikacji	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Wykrywanie automatyczne i instalacja zdalna			
Wykrywanie w sieci	Tak	Nie	Nie
Wykrywanie w domenie Active Directory	Tak	Nie	Nie
Wykrywanie w szablonach (import maszyn z pliku)	Tak	Nie	Nie
Ręczne dodawanie urządzeń	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Active Protection			
Wykrywanie wstrzyknięć procesów	Tak	Nie	Nie
Automatycznie odzyskiwanie plików, których dotyczy problem, z lokalnej pamięci podręcznej	Tak	Tak	Tak
Samoobrona plików kopii zapasowych Acronis	Tak	Nie	Nie
Samoobrona oprogramowania Acronis	Tak	Nie	Tak (Tylko komponenty Active Protection i

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Active Protection			
			Ochrona przed złośliwym oprogramowaniem)
Zarządzanie zaufanymi/zablokowanymi procesami	Tak	Nie	Tak
Wykluczanie procesów/folderów	Tak	Tak	Tak
Wykrywanie oprogramowania wymuszającego okup na podstawie zachowań procesów (przy użyciu sztucznej inteligencji)	Tak	Tak	Tak
Wykrywanie procesów cryptominingu na podstawie ich zachowań	Tak	Nie	Nie
Ochrona dysków zewnętrznych (HDD, pamięć flash USB, karty SD)	Tak	Nie	Tak
Ochrona folderów sieciowych	Tak	Tak	Tak
Ochrona po stronie serwera	Tak	Nie	Nie
Ochrona programów Zoom, Cisco Webex, Citrix Workspace i Microsoft Teams	Tak	Nie	Nie
Dodatkowe informacje na temat obsługiwanych systemów operacyjnych i ich wersji można znaleźć w sekcji "Obsługiwane platformy" (s. 875).			

Zestaw funkcji	Windows	Linux	macOS
Ochrona przed wirusami i złośliwym oprogramowaniem			
W pełni zintegrowana funkcja Active Protection	Tak	Nie	Nie
Ochrona antywirusowa w czasie rzeczywistym	Tak	Tak, z pakietem Zaawansowana ochrona przed złośliwym oprogramowaniem	Tak, z pakietem Zaawansowana ochrona przed złośliwym oprogramowaniem
Zaawansowana ochrona przed złośliwym oprogramowaniem w czasie rzeczywistym z lokalnym wykrywaniem plików opartym na sygnaturach	Tak	Tak	Tak

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Ochrona przed wirusami i złośliwym oprogramowaniem			
Statyczne analizy przenośnych plików wykonywalnych	Tak	Nie	Tak*
Skanowanie antywirusowe na żądanie	Tak	Tak**	Tak
Ochrona folderów sieciowych	Tak	Tak	Nie
Ochrona po stronie serwera	Tak	Nie	Nie
Skanowanie plików archiwum	Tak	Nie	Tak
Skanowanie dysków wymiennych	Tak	Nie	Tak
Skanowanie tylko nowych i zmienionych plików	Tak	Nie	Tak
Wykluczanie plików/folderów	Tak	Tak	Tak***
Wykluczanie procesów	Tak	Nie	Tak
Mechanizm analiz zachowań	Tak	Nie	Tak
Ochrona przed exploitami	Tak	Nie	Nie
Kwarantanna	Tak	Tak	Tak
Automatyczne czyszczenie kwarantanny	Tak	Tak	Tak
Filtrowanie adresów URL (http/https)	Tak	Nie	Nie
Ogólnofirmowa biała lista	Tak	Nie	Tak
Zarządzanie zaporą****	Tak	Nie	Nie
Zarządzanie programem Microsoft Defender Antivirus*****	Tak	Nie	Nie
Zarządzanie programem Microsoft Security Essentials	Tak	Nie	Nie
Rejestrowanie modułu Ochrona przed wirusami i złośliwym oprogramowaniem oraz zarządzanie nim za pośrednictwem Centrum zabezpieczeń systemu	Tak	Nie	Nie

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Ochrona przed wirusami i złośliwym oprogramowaniem			
Windows			
Dodatkowe informacje na temat obsługiwanych systemów operacyjnych i ich wersji można znaleźć w sekcji "Obsługiwane platformy" (s. 875).			

* Statyczne analizy przenośnych plików wykonywalnych są obsługiwane tylko w przypadku planowanych operacji skanowania w systemie macOS.

** Warunki uruchomienia nie są obsługiwane w przypadku skanowania na żądanie w systemie Linux.

*** Wykluczanie plików/folderów jest obsługiwane tylko w przypadku wskazania plików i folderów, które nie będą skanowane w ramach ochrony w czasie rzeczywistym ani planowanych operacji skanowania w systemie macOS.

**** Zarządzenie zaporą jest dostępne w systemie Windows 8 lub nowszym. System Windows Server nie jest obsługiwany.

***** Zarządzanie programem Microsoft Defender Antivirus jest obsługiwane w systemie Windows 8.1 lub nowszym.

Zestaw funkcji	Windows	Linux	macOS
Ocena luk w zabezpieczeniach			
Ocena luk w zabezpieczeniach systemu operacyjnego i jego macierzystych aplikacji	Tak	Tak******	Tak
Ocena luk w zabezpieczeniach aplikacji innych firm	Tak	Nie	Tak
Dodatkowe informacje na temat obsługiwanych systemów operacyjnych i ich wersji można znaleźć w sekcjach "Obsługiwane produkty firmy Microsoft i innych firm" (s. 1035), "Obsługiwane produkty dla systemu Linux" (s. 1037) i "Obsługiwane produkty firmy Apple i innych firm" (s. 1036).			

****** Ocena luk w zabezpieczeniach zależy od dostępności oficjalnych ostrzeżeń dotyczących bezpieczeństwa dla danej dystrybucji, na przykład https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce i innych.

Zestaw funkcji	Windows	Linux	macOS
Zarządzanie poprawkami			
Automatyczne zatwierdzanie poprawek	Tak	Nie	Nie
Automatyczna instalacja poprawek	Tak	Nie	Nie
Testowanie poprawek	Tak	Nie	Nie

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Zarządzanie poprawkami			
Ręczna instalacja poprawek	Tak	Nie	Nie
Planowanie poprawek	Tak	Nie	Nie
Bezpieczne wdrażanie poprawek: utworzenie kopii zapasowej komputera przed instalacją poprawki w ramach planu ochrony	Tak	Nie	Nie
Anulowanie ponownego uruchomienia komputera podczas operacji tworzenia kopii zapasowej	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Funkcje	Windows	Linux	macOS
Mapa ochrony danych			
Dostosowywana definicja ważnych plików	Tak	Nie	Nie
Skanowanie komputerów w poszukiwaniu niechronionych plików	Tak	Nie	Nie
Przegląd niechronionych lokalizacji	Tak	Nie	Nie
Możliwość uruchomienia działań ochronnych z widżetu Mapa ochrony danych (działanie **Chroń wszystkie pliki**)	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Kondycje dysków			
Kontrola kondycji dysków HDD i SSD przy użyciu sztucznej inteligencji	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Funkcje	Windows	Linux	macOS
Inteligentne plany ochrony oparte na ostrzeżeniach z Acronis Cyber Protection Operations Center (CPOC)			
Kanał dotyczący zagrożeń	Tak	Nie	Nie

© Acronis International GmbH, 2003-2024

Funkcje	Windows	Linux	macOS
Inteligentne plany ochrony oparte na ostrzeżeniach z Acronis Cyber Protection Operations Center (CPOC)			
Kreator napraw	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Skanowanie kopii zapasowych			
Skanowanie antywirusowe kopii zapasowych obrazów w ramach planu tworzenia kopii zapasowych	Tak	Nie	Nie
Skanowanie antywirusowe kopii zapasowych obrazów w chmurze	Tak	Nie	Nie
Skanowanie antywirusowe zaszyfrowanych kopii zapasowych	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Bezpieczne odzyskiwanie			
Skanowanie przy użyciu modułu Ochrona przed wirusami i złośliwym oprogramowaniem podczas odzyskiwania	Tak	Nie	Nie
Bezpieczne odzyskiwanie zaszyfrowanych kopii zapasowych	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Połączenie pulpitu zdalnego			
Połączenie przy użyciu protokołu NEAR	Tak	Tak	Tak
Połączenie przy użyciu protokołu RDP	Tak	Nie	Nie
Połączenie przez Udostępnianie ekranu firmy Apple	Nie	Nie	Tak
Połączenie przy użyciu klienta internetowego	Tak	Nie	Nie
Połączenie przy użyciu aplikacji Quick Assist	Tak	Tak	Tak

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Połączenie pulpitu zdalnego			
Pomoc zdalna	Tak	Tak	Tak
Przesyłanie plików	Tak	Tak	Tak
Przesyłanie zrzutu ekranu	Tak	Tak	Tak
Dodatkowe informacje na temat obsługiwanych systemów operacyjnych i ich wersji można znaleźć w sekcji "Obsługiwane platformy" (s. 1077).			

Zestaw funkcji	Windows	Linux	macOS
Wynik #CyberFit			
Status wyniku #CyberFit	Tak	Nie	Nie
Autonomiczne narzędzie Wynik #CyberFit	Tak	Nie	Nie
Zalecenia dotyczące Wyniku #CyberFit	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Ochrona przed utratą danych			
Kontrola urządzeń	Tak	Nie	Obsługiwane na komputerach Mac z procesorami Intel i systemem macOS w wersji 10.15 lub nowszej albo macOS w wersji 11.2.3 lub nowszej. Nie jest obsługiwane w przypadku procesorów Apple Silicon opartych na architekturze ARM, takich jak

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Ochrona przed utratą danych			
			Apple M1 / M2.
Advanced Data Loss Prevention	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47).			

Zestaw funkcji	Windows	Linux	macOS
Opcje zarządzania			
Scenariusze sprzedaży dodatkowej do promowania różnych wersji programu Cyber Protect	Tak	Tak	Tak
Konsola internetowa do zarządzania scentralizowanego i zdalnego	Tak	Tak	Tak
Obsługiwane systemy operacyjne i wersje: Niezależnie od platformy.			

Zestaw funkcji	Windows	Linux	macOS
Opcje ochrony			
Wymazywanie zdalne	Tak	Nie	Nie
Obsługiwane w przypadku systemu Windows w wersji 10 lub nowszej.			

Zestaw funkcji	Windows	Linux	macOS
Cyber Protect Monitor			
Aplikacja Cyber Protect	Tak	Nie	Tak
Status ochrony programu Zoom	Tak	Nie	Nie
Status ochrony programu Cisco Webex	Tak	Nie	Nie
Status ochrony programu Citrix Workspace	Tak	Nie	Nie
Status ochrony programu Microsoft Teams	Tak	Nie	Nie
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47). Funkcja Cyber Protect Monitor jest obsługiwana we wszystkich wersjach, w których można zainstalować agenta dla systemu Mac. Aby uzyskać więcej informacji, zobacz "Agent dla systemu Mac" (s. 28).			

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Inwentaryzacja oprogramowania			
Skanowanie na potrzeby inwentaryzacji oprogramowania	Tak	Nie	Tak
Monitorowanie inwentaryzacji oprogramowania	Tak	Nie	Tak
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47). Inwentaryzacja oprogramowania jest obsługiwana w systemach macOS 10.13.x–13.x.			

Zestaw funkcji	Windows	Linux	macOS
Inwentaryzacja sprzętu			
Skanowanie w celu inwentaryzacji sprzętu	Tak	Nie	Tak
Monitorowanie inwentaryzacji sprzętu	Tak	Nie	Tak
Obsługiwane wersje systemu Windows można sprawdzić w sekcji "Obsługiwane systemy operacyjne i wersje" (s. 47). Inwentaryzacja sprzętu jest obsługiwana w systemach macOS 10.13.x–13.x.			

Obsługiwane systemy plików

Agent ochrony może tworzyć kopie zapasowe każdego systemu plików dostępnego z systemu operacyjnego, w którym ten agent jest zainstalowany. Na przykład agent dla systemu Windows może tworzyć kopie zapasowe systemu plików ext4 i go odzyskiwać, jeśli w systemie Windows jest zainstalowany odpowiedni sterownik.

W poniższej tabeli zestawiono systemy plików, które można uwzględniać w kopiach zapasowych i odzyskiwać (nośnik startowy obsługuje tylko odzyskiwanie). Ograniczenia dotyczą zarówno agentów, jak i nośnika startowego.

System plików	Obsługujące agenty i nośniki			Ograniczenia
	Agenty	Nośnik startowy dla systemu Windows i Linux	Nośnik startowy dla systemu Mac	
FAT16/32	Wszystkie agenty	+	+	Brak ograniczeń
NTFS	Wszystkie	+	+	

© Acronis International GmbH, 2003-2024

System plików	Obsługujące agenty i nośniki			Ograniczenia
	Agenty	Nośnik startowy dla systemu Windows i Linux	Nośnik startowy dla systemu Mac	
	agenty			
ext2/ext3/ext4	Wszystkie agenty	+	-	
HFS+	Agent dla systemu Mac	-	+	
APFS	Agent dla systemu Mac	-	+	• Obsługiwany od wersji macOS High Sierra 10.13 • W przypadku odzyskiwania na komputer inny niż oryginalny lub komputer bez systemu operacyjnego należy ręcznie odtworzyć konfigurację dysków.
JFS	Agent dla systemu Linux	+	-	• Filtry plików (uwzględniające/wykluczające) nie są obsługiwane • Nie można włączyć opcji tworzenia szybkiej przyrostowej/różnicowej kopii zapasowej
ReiserFS3	Agent dla systemu Linux	+	-	
ReiserFS4	Agent dla systemu Linux	+	-	• Filtry plików (uwzględniające/wykluczające) nie są obsługiwane • Nie można włączyć opcji tworzenia szybkiej przyrostowej/różnicowej kopii zapasowej • Podczas odzyskiwania nie można zmieniać rozmiarów woluminów
ReFS	Wszystkie agenty	+	+	• Filtry plików (uwzględniające/wykluczające) nie są obsługiwane

© Acronis International GmbH, 2003-2024

System plików	Obsługujące agenty i nośniki			Ograniczenia
	Agenty	Nośnik startowy dla systemu Windows i Linux	Nośnik startowy dla systemu Mac	
				• Nie można włączyć opcji tworzenia szybkiej przyrostowej/różnicowej kopii zapasowej • Podczas odzyskiwania nie można zmieniać rozmiarów woluminów • W przypadku odzyskiwania plików z kopii zapasowej systemu plików ReFS odzyskiwana jest tylko zawartość. Listy kontroli dostępu (ACL) i strumienie alternatywne nie są odzyskiwane. Pliki rozrzedzone są odzyskiwane jako zwykłe pliki.
XFS	Wszystkie agenty	+	+	• Filtry plików (uwzględniające/wykluczające) nie są obsługiwane • Nie można włączyć opcji tworzenia szybkiej przyrostowej/różnicowej kopii zapasowej • Podczas odzyskiwania nie można zmieniać rozmiarów woluminów • Tryb szybkiej przyrostowej kopii zapasowej nie jest obsługiwany w przypadku systemu plików XFS. Operacje tworzenia przyrostowych i różnicowych kopii zapasowych woluminów XFS w chmurze mogą trwać znacznie dłużej niż porównywalne operacje tworzenia kopii zapasowych

© Acronis International GmbH, 2003-2024

System plików	Obsługujące agenty i nośniki			Ograniczenia
	Agenty	Nośnik startowy dla systemu Windows i Linux	Nośnik startowy dla systemu Mac	
				w systemie ext4, w których jest stosowany tryb szybkiej przyrostowej kopii zapasowej.
Linux Swap	Agent dla systemu Linux	+	-	Brak ograniczeń
exFAT	Wszystkie agenty	+ Jeśli kopia zapasowa *jest przechowywana* w systemie plików exFAT, nie można przeprowadzić odzyskiwania przy użyciu nośnika startowego	+	• Obsługiwana jest wyłącznie kopia zapasowa dysku/woluminu • Filtry plików (uwzględniające/wykluczające) nie są obsługiwane • Nie można odzyskiwać poszczególnych plików z kopii zapasowej

W przypadku tworzenia kopii zapasowej dysku z nierozpoznanym lub nieobsługiwanym systemem plików (na przykład Btrfs) oprogramowanie automatycznie przełącza się na tryb „sektor po sektorze". Kopię zapasową sektor po sektorze można utworzyć w przypadku każdego systemu plików, który spełnia następujące warunki:

- jest oparty na blokach
- obejmuje jeden dysk
- ma standardowy schemat partycjonowania MBR/GPT

Jeśli system plików nie spełnia tych wymagań, operacja tworzenia kopii zapasowej się nie powiedzie.

Deduplikacja danych

W systemie Windows Server 2012 lub nowszym można włączyć funkcję deduplikacji danych w przypadku woluminu NTFS. Deduplikacja danych zmniejsza ilość zużytego miejsca na woluminie dzięki jednokrotnemu zapisywaniu zduplikowanych na woluminie fragmentów plików.

© Acronis International GmbH, 2003-2024

W przypadku woluminów z włączoną funkcją deduplikacji danych można bez ograniczeń używać funkcji tworzenia kopii zapasowych na poziomie dysku oraz ich odzyskiwania. Tworzenie kopii zapasowych na poziomie plików jest obsługiwane, z wyjątkiem sytuacji, gdy jest używany komponent Acronis VSS Provider. Aby odzyskać pliki z kopii zapasowej dysku, uruchom maszynę wirtualną z kopii zapasowej lub zamontuj kopię zapasową na komputerze z systemem operacyjnym Windows Server 2012 lub nowszym, a następnie skopiuj pliki z zamontowanego woluminu.

Funkcja deduplikacji danych systemu Windows Server nie jest związana z funkcją Acronis Backup Deduplication.

Obsługiwane operacje na woluminach logicznych

Tworzenie kopii zapasowych i odzyskiwanie maszyn z woluminami logicznymi, takimi jak LDM w systemie Windows (dyski dynamiczne) i LVM w systemie Linux, jest obsługiwane z następującymi ograniczeniami.

Kopia zapasowa

Kopia zapasowa tworzona za pomocą agenta to kopia zapasowa tworzona przez agenta ochrony zainstalowanego na maszynie lub nośniku startowym.

Bezagentowe tworzenie kopii zapasowych jest dostępne tylko w przypadku maszyn wirtualnych. Bezagentowe tworzenie kopii zapasowych jest wykonywane na poziomie hiperwizora przez agenta, który może tworzyć kopie zapasowe wszystkich maszyn wirtualnych w środowisku i je odzyskiwać. Nie instaluje się osobnych agentów na chronionych maszynach wirtualnych.

Więcej informacji na temat różnic między operacjami tworzenia kopii zapasowych za pomocą agenta a operacjami tworzenia kopii zapasowych bezagentowo można znaleźć w sekcji "Tworzenie kopii zapasowych przy użyciu agenta i bezagentowe" (s. 66).

Kopia zapasowa utworzona przy użyciu agenta	Kopia zapasowa utworzona bezagentowo
• W przypadku woluminów logicznych są tworzone kopie zapasowe każdego woluminu z osobna. • Obsługiwane są (uwzględniające i wykluczające) filtry plików.	• W przypadku wykrycia woluminu logicznego na dysku kopia zapasowa dysku jest tworzona w trybie sektor po sektorze (RAW). Nie jest analizowana struktura partycji dysku i nie są osobno zapisywane żadne obrazy woluminów. • Nie można wybrać pojedynczych woluminów LDM lub LVM jako źródła kopii zapasowej — ani bezpośrednio, ani przy użyciu reguł zasad. W sekcji **Elementy do uwzględnienia w kopii zapasowej** planu ochrony dostępna jest tylko opcja **Cały komputer**. • Filtry plików (uwzględniające/wykluczające) nie są obsługiwane. Wszelkie skonfigurowane uwzględnienia lub wykluczenia zostaną zignorowane.

© Acronis International GmbH, 2003-2024

Odzyskiwanie

Odzyskiwanie za pomocą agenta oznacza operację odzyskiwania wykonywaną przez agenta zainstalowanego na maszynie lub nośniku startowym.

Odzyskiwanie bezagentowe jest obsługiwane wyłącznie w przypadku maszyn wirtualnych jako lokalizacji docelowych. Odzyskiwanie bezagentowe jest wykonywane na poziomie hiperwizora przez agenta, który może tworzyć kopie zapasowe i odtwarzać wszystkie maszyny wirtualne w środowisku. Nie trzeba ręcznie tworzyć komputera docelowego, na który będzie odzyskiwana kopia zapasowa.

	Z kopii zapasowej utworzonej przy użyciu agenta	**Z kopii zapasowej utworzonej bezagentowo**
Odzyskiwanie przy użyciu agenta	• Odzyskiwanie poszczególnych woluminów jest dostępne. • Odzyskiwanie plików i folderów jest dostępne.	• Odzyskiwanie poszczególnych woluminów nie jest dostępne. • Odzyskiwanie plików i folderów jest dostępne.
Odzyskiwanie bezagentowe	• Migracja maszyn (P2V, V2P i V2V) nie jest obsługiwana. Aby odzyskać dane z kopii zapasowej utworzonej przy użyciu agenta, użyj nośnika startowego. • Operacja **Uruchom jako maszynę wirtualną** nie jest obsługiwana. • Odzyskiwanie plików i folderów jest dostępne.	• Odzyskiwanie poszczególnych woluminów nie jest dostępne. • Odzyskiwanie całego komputera jest dostępne. • Odzyskiwanie plików i folderów jest dostępne. • Operacja **Uruchom jako maszynę wirtualną** jest obsługiwana. Aby móc uruchomić maszynę wirtualną, może być konieczna zmiana kolejności rozruchu. Więcej informacji można znaleźć w tym artykule bazy wiedzy. • Obsługiwana jest konwersja na następujące typy maszyn wirtualnych: ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

© Acronis International GmbH, 2003-2024

Instalowanie i wdrażanie agentów Cyber Protection

Zanim zaczniesz

Przygotowanie

Krok 1

Wybierz agenta w zależności od elementów, których kopię zapasową zamierzasz utworzyć. Więcej informacji na temat możliwych wyborów można znaleźć w sekcji Który agent jest potrzebny?

Krok 2

Upewnij się, że na dysku twardym jest wystarczająco dużo wolnego miejsca, aby można było zainstalować agenta. Szczegółowe informacje na temat wymaganego miejsca można znaleźć w sekcji "Wymagania systemowe agentów" (s. 71).

Krok 3

Pobierz program instalacyjny. Aby znaleźć łącza pobierania, kliknij **Wszystkie urządzenia** > **Dodaj**.

Na stronie **Dodaj urządzenia** są dostępne instalatory internetowe każdego agenta instalowanego w systemie Windows. Instalator internetowy jest małym plikiem wykonywalnym, który pobiera główny program instalacyjny z Internetu i zapisuje go jako plik tymczasowy. Plik ten jest usuwany natychmiast po zakończeniu instalacji.

Jeśli chcesz przechowywać programy instalacyjne lokalnie, pobierz pakiet zawierający wszystkie agenty do instalacji w systemie Windows, korzystając z łącza dostępnego u dołu strony **Dodaj urządzenia**. Pakiet jest dostępny w wersji zarówno 32-, jak i 64-bitowej. Pakiety te umożliwiają dostosowanie listy komponentów do zainstalowania. Pakiet umożliwia instalację nienadzorowaną, na przykład przy użyciu zasad grupy. Ten zaawansowany scenariusz opisano tutaj: "Wdrażanie agentów ochrony przy użyciu zasad grupy" (s. 143).

Aby pobrać program instalacyjny agenta dla usługi Microsoft 365, kliknij ikonę konta w prawym górnym rogu, a następnie kliknij **Do pobrania** > **Agent dla usługi Microsoft 365**.

W systemach Linux i macOS instalację wykonuje się przy użyciu zwykłych programów instalacyjnych.

Wszystkie programy instalacyjne wymagają połączenia z Internetem w celu rejestracji komputera w usłudze Cyber Protection. W przypadku braku połączenia z Internetem instalacja się nie powiedzie.

Krok 4

Funkcje usługi Cyber Protect wymagają pakietu redystrybucyjnego Microsoft Visual C++ 2017. Sprawdź, czy jest on już zainstalowany na komputerze, i ewentualnie zainstaluj go przed

© Acronis International GmbH, 2003-2024

zainstalowaniem agenta. Po zainstalowaniu pakietu Microsoft Visual C++ może być wymagane ponowne uruchomienie komputera. Pakiet redystrybucyjny Microsoft Visual C++ jest dostępny tutaj: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Krok 5

Upewnij się, że zapory i inne komponenty systemu zabezpieczeń sieci (np. serwer proxy) umożliwiają połączenia wychodzące przez poniższe porty TCP.

- Porty **443** i **8443**

  Porty te służą do uzyskiwania dostępu do konsoli Cyber Protect, rejestrowania agentów, pobierania certyfikatów, autoryzacji użytkowników oraz pobierania plików z chmury.
- Porty w zakresie **7770**–**7800**

  Agenty używają tych portów do komunikacji z serwerem zarządzania.
- Porty **44445** i **55556**

  Agenty używają tych portów do przesyłania danych podczas tworzenia kopii zapasowych i odzyskiwania.

Jeśli w danej sieci jest włączony serwer proxy, zajrzyj do sekcji „"Konfigurowanie ustawień serwera proxy" (s. 78)”, aby sprawdzić, czy trzeba skonfigurować te ustawienia na każdym komputerze, na którym działa agent ochrony.

Minimalna prędkość łącza internetowego niezbędna do zarządzania agentem z chmury to 1 Mb/s (nie mylić z minimalną prędkością transmisji danych do tworzenia kopii zapasowych w chmurze). Należy o tym pamiętać w przypadku korzystania z połączeń o niskiej przepustowości, na przykład ADSL.

Porty TCP wymagane do operacji tworzenia kopii zapasowych i replikacji maszyn wirtualnych VMware

- Port **443**

  Agent dla VMware (zarówno Windows, jak i urządzenie wirtualne) łączy się z tym portem hosta ESXi lub serwera vCenter w celu wykonania operacji zarządzania maszynami wirtualnymi, takich jak utworzenie, aktualizacja i usunięcie maszyn wirtualnych w vSphere podczas operacji tworzenia kopii zapasowych, odzyskiwania oraz replikacji maszyn wirtualnych.
- Port **902**

  Agent dla VMware (zarówno Windows, jak i urządzenie wirtualne) łączy się z tym portem hosta ESXi w celu ustanowienia połączenia NFC na potrzeby odczytu/zapisu danych na maszynach wirtualnych podczas operacji tworzenia kopii zapasowych, odzyskiwania i replikacji maszyn wirtualnych.
- Port **3333**

  Jeśli agent dla VMware (urządzenie wirtualne) działa na hoście/klastrze ESXi, który jest obiektem docelowym replikacji maszyny wirtualnej, ruch związany z replikacją maszyny wirtualnej nie trafia bezpośrednio do hosta ESXi na port **902**. Zamiast tego ruch trafia od źródłowego agenta dla

© Acronis International GmbH, 2003-2024

VMware na port TCP **3333** agenta dla VMware (urządzenie wirtualne) znajdującego się na docelowym hoście/klastrze ESXi.

Źródłowy agent dla VMware, który odczytuje dane z oryginalnych dysków VM, może się znajdować w dowolnym miejscu i być dowolnego typu: urządzenie wirtualne lub Windows.

Usługa, która odpowiada za przyjmowanie danych replikacji maszyny wirtualnej w docelowym agencie dla VMware (urządzenie wirtualne), nosi nazwę „Serwer dysków replik". Usługa ta odpowiada za techniki optymalizacji sieci WAN, takie jak kompresja ruchu i deduplikacja podczas replikacji maszyn wirtualnych, w tym seeding replik (zobacz Seeding repliki początkowej).W sytuacji, gdy na docelowym hoście ESXi nie działa agent dla VMware (urządzenie wirtualne), usługa ta nie jest dostępna, w związku z czym scenariusz seedingu replik nie jest obsługiwany.

Porty wymagane przez komponent Menedżer pobierania

Komponent Menedżer pobierania odpowiada za dostarczanie aktualizacji na komputer i rozpowszechnianie ich wśród innych instancji Menedżera pobierania. Może on działać w trybie agenta, w którym komputer staje się agentem Menedżera pobierania. Agent Menedżera pobierania pobiera aktualizacje z Internetu i serwerów, używając ich jako źródła aktualizacji rozpowszechnianych wśród kolejnych komputerów. Menedżer pobierania wymaga do działania następujących portów:

- Port TCP i UDP (przychodzące) **6888**

  Port używany przez protokół BitTorrent na potrzeby aktualizacji torrentów w komunikacji równorzędnej (peer-to-peer).
- Port UDP **6771**

  Port do wykrywania lokalnych komputerów równorzędnych (pear). Port ten jest używany również na potrzeby aktualizacji w komunikacji równorzędnej (peer-to-peer).
- Port TCP **18018**

  Port używany do komunikacji między aktualizatorami działającymi w różnych trybach: Aktualizator i Agent aktualizatora.
- Port TCP **18019**

  Port lokalny używany do komunikacji między aktualizatorem a agentem ochrony.

Krok 6

Sprawdź, czy na komputerze, na którym planujesz zainstalować agenta ochrony, inne procesy nie używają poniższych portów lokalnych.

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**
- 127.0.0.1:**9850**

Uwaga
Nie trzeba ich otwierać na zaporze.

© Acronis International GmbH, 2003-2024

Zmienianie portów używanych przez agenta ochrony

Niektóre porty wymagane przez agenta ochrony mogą być używane przez inne aplikacje w środowisku. Aby uniknąć konfliktów, można zmienić domyślne porty używane przez agenta ochrony, modyfikując następujące pliki.

- W systemie Linux: `/opt/Acronis/etc/aakore.yaml`
- W systemie Windows: `\ProgramData\Acronis\Agent\etc\aakore.yaml`

Tworzenie kopii zapasowych przy użyciu agenta i bezagentowe

Tworzenie kopii zapasowych przy użyciu agenta wymaga zainstalowania agenta ochrony na każdym chronionym komputerze. Tworzenie kopii zapasowych przy użyciu agenta jest obsługiwane na wszystkich komputerach fizycznych i maszynach wirtualnych. Dodatkowe informacje na temat potrzebnego agenta i miejsca jego instalacji można znaleźć w sekcji "Który agent jest potrzebny?" (s. 67)

Bezagentowe tworzenie kopii zapasowych jest obsługiwane przez niektóre platformy wirtualizacji — nie jest dostępne w przypadku komputerów fizycznych. Bezagentowe tworzenie kopii zapasowych wymaga tylko jednego agenta ochrony, zainstalowanego na wyznaczonej do tego celu maszynie w środowisku wirtualnym. Agent ten tworzy kopie zapasowe pozostałych maszyn wirtualnych w tym środowisku. Aby uzyskać więcej informacji na temat obsługiwanych typów kopii zapasowych na poszczególnych platformach wirtualizacji, zobacz sekcję "Obsługiwane platformy wirtualizacji" (s. 32).

W przypadku niektórych platform wirtualizacji dostępne są urządzenia wirtualne. Urządzenie wirtualne to gotowa maszyna wirtualna, która już zawiera agenta ochrony. Urządzenia wirtualne są dostępne w formatach odpowiednich dla hiperwizora, takich jak .ovf, .ova lub .qcow.

Jakiego typu kopii zapasowej potrzebuję?

Zalecamy tworzenie kopii zapasowych za pomocą agenta, jeśli w środowisku są potrzebne:

- Dodatkowe funkcje ochrony, takie jak ochrona przed wirusami i złośliwym oprogramowaniem, zarządzanie poprawkami lub połączenie pulpitu zdalnego. Aby uzyskać więcej informacji na temat tych funkcji, zobacz sekcję "Obsługa funkcji ochrony w poszczególnych systemach operacyjnych" (s. 47).
- Osobne maszyny wirtualne na poziomie dzierżawcy. Na przykład wtedy, gdy użytkownicy w ramach dzierżawcy mają mieć dostęp tylko do własnych kopii zapasowych.
- Kopie zapasowe na poziomie plików, które można odzyskiwać w systemach operacyjnych gości.

Zalecamy bezagentowe tworzenie kopii zapasowych, jeśli w środowisku są potrzebne:

- Tylko kopia zapasowa, bez żadnych dodatkowych funkcji ochrony.
- Uproszczone zarządzanie — możesz tworzyć kopie zapasowe wielu maszyn wirtualnych po zainstalowaniu i skonfigurowaniu zaledwie jednego agenta.

© Acronis International GmbH, 2003-2024

- Minimalne zużycie zasobów — jeden dedykowany agent zużywa mniej procesora i pamięci RAM niż wiele agentów zainstalowanych na każdej maszynie wirtualnej w środowisku.
- Konkretne konfiguracje kopii zapasowych, na przykład operacji tworzenia kopii zapasowych bez obciążania sieci lokalnej. Aby uzyskać więcej informacji na temat tej funkcji, zobacz sekcję "Agent dla VMware — tworzenie kopii zapasowych bez obciążania sieci lokalnej" (s. 735).
- Mniejsze obciążenie konfiguracyjne. Dedykowany agent tworzy kopie zapasowe maszyn wirtualnych na poziomie hiperwizora, niezależnie od systemów operacyjnych gości.

Który agent jest potrzebny?

Wybór agenta zależy od elementów, których kopię zapasową zamierzasz utworzyć. Poniższa tabela zawiera zestawienie informacji ułatwiających decyzję.

W przypadku instalacji w systemie agent dla programu Exchange, agent dla SQL, agent dla usługi Active Directory oraz agent dla programu Oracle wymagają zainstalowania również agenta dla systemu Windows. Dzięki temu po zainstalowaniu na przykład agenta dla SQL można utworzyć kopię zapasową całego komputera, na którym został zainstalowany ten agent.

W przypadku instalowania agenta dla VMware (Windows) i agenta dla Hyper-V zalecamy zainstalowanie również agenta dla systemu Windows.

W systemie Linux agent dla programu Oracle, agent dla MySQL/MariaDB i agent dla Virtuozzo wymagają zainstalowania również agenta dla systemu Linux (64-bitowego). Agenty te są uwzględnione w pliku instalacyjnym agenta dla systemu Linux (wersja 64-bitowa).

Co chcesz uwzględnić w kopii zapasowej?	Którego agenta należy zainstalować?	Gdzie trzeba go zainstalować?
Komputery fizyczne		
Komputery fizyczne z systemem Windows	Agent dla systemu Windows	Na komputerze, którego kopia zapasowa jest tworzona.
Komputery fizyczne z systemem Linux	Agent dla systemu Linux	
Komputery fizyczne z systemem macOS	Agent dla systemu Mac	
Bazy danych		
Bazy danych SQL	Agent dla SQL	Na komputerze z programem Microsoft SQL Server.
Bazy danych MySQL	Agent dla MySQL/MariaDB	Na komputerze z działającym

© Acronis International GmbH, 2003-2024

	[Uwzględniony w pliku instalacyjnym agenta dla systemu Linux (wersja 64-bitowa)]	rozwiązaniem MySQL Server.
Bazy danych MariaDB	Agent dla MySQL/MariaDB [Uwzględniony w pliku instalacyjnym agenta dla systemu Linux (wersja 64-bitowa)]	Na komputerze z działającym rozwiązaniem MariaDB Server.
Bazy danych programu Exchange	Agent dla programu Exchange	Na komputerze z rolą Skrzynka pocztowa programu Microsoft Exchange Server*.
Bazy danych Oracle	Agent dla programu Oracle [W systemie Linux uwzględniony w pliku instalacyjnym agenta dla systemu Linux (wersja 64-bitowa)]	Na komputerze z systemem Oracle Database.
Obciążenia międzychmurowe		
Skrzynki pocztowe Microsoft 365 (Agent w chmurze lub agent lokalny)	Agent w chmurze (Nie jest wymagana żadna instalacja)	Ta funkcja jest udostępniana wraz z agentem w chmurze wdrażanym w centrum danych. Aby uzyskać więcej informacji, zobacz "Przy użyciu chmurowego agenta dla usługi Microsoft 365" (s. 651).
	Agent dla usługi Office 365	Na podłączonym do Internetu komputerze z systemem Windows. Aby uzyskać więcej

© Acronis International GmbH, 2003-2024

		informacji, zobacz "Korzystanie z zainstalowanego lokalnie agenta dla Office 365" (s. 647).
Pliki Microsoft 365 OneDrive oraz witryny SharePoint Online	Agent w chmurze (Nie jest wymagana żadna instalacja)	Ta funkcja jest udostępniana wraz z agentem w chmurze wdrażanym w centrum danych. Aby uzyskać więcej informacji, zobacz "Przy użyciu chmurowego agenta dla usługi Microsoft 365" (s. 651).
Dane pakietu Google Workspace — skrzynki pocztowe Gmail, pliki z Dysku Google i pliki z Dysku udostępnionego	Agent w chmurze (Nie jest wymagana żadna instalacja)	Ta funkcja jest udostępniana wraz z agentem w chmurze wdrażanym w centrum danych. Aby uzyskać więcej informacji, zobacz "Ochrona danych pakietu Google Workspace" (s. 686).
Active Directory		
Komputery z usługami domenowymi Active Directory	Agent dla usługi Active Directory	Na kontrolerze domeny.
Maszyny wirtualne		
Maszyny wirtualne VMware ESXi	Agent dla VMware (Windows)	Na komputerze z systemem Windows, który ma dostęp przez sieć do serwera vCenter oraz magazynu maszyn wirtualnych**.
	Agent dla VMware (urządzenie wirtualne)	Na hoście ESXi.

© Acronis International GmbH, 2003-2024

Maszyny wirtualne Hyper-V	Agent dla Hyper-V	Na hoście Hyper-V.
Maszyny wirtualne Scale Computing HC3	Agent dla Scale Computing HC3 (urządzenie wirtualne)	Na hoście Scale Computing HC3.
Maszyny wirtualne Red Hat Virtualization (zarządzane przez oVirt)	Agent dla oVirt (urządzenie wirtualne)	Na hoście Red Hat Virtualization.
Maszyny wirtualne i kontenery Virtuozzo***	Agent dla Virtuozzo [Uwzględniony w pliku instalacyjnym agenta dla systemu Linux (wersja 64-bitowa)]	Na hoście Virtuozzo.
Maszyny wirtualne Virtuozzo Hybrid Infrastructure	Agent dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne)	Na hoście Virtuozzo Hybrid Infrastructure.
Maszyny wirtualne znajdujące się w środowisku Amazon EC2	Taki sam jak na komputerze fizycznym****	Na komputerze, którego kopia zapasowa jest tworzona.
Maszyny wirtualne znajdujące się w środowisku Windows Azure		
Maszyny wirtualne Citrix XenServer		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
Środowiska Kernel-based Virtual Machine (KVM), niezarządzane przez oVirt		
Maszyny wirtualne Oracle, niezarządzane przez oVirt		
Maszyny wirtualne Nutanix AHV		
Red Hat Virtualization (RHV/RHEV), zarządzane przez oVirt	Agent dla oVirt (urządzenie wirtualne)	Na hoście wirtualizacji.
Środowiska Kernel-based Virtual Machine (KVM), zarządzane przez oVirt		
Maszyny wirtualne Oracle, zarządzane przez oVirt		
Urządzenia mobilne		
Urządzenia mobilne z systemem Android	Aplikacja mobilna dla systemu Android	Na urządzeniu mobilnym, którego

© Acronis International GmbH, 2003-2024

Urządzenia mobilne z systemem iOS	Aplikacja mobilna dla systemu iOS	kopia zapasowa zostanie utworzona.

* Podczas instalacji agent dla programu Exchange sprawdza, czy na komputerze, na którym będzie uruchamiany, jest wystarczająco dużo wolnego miejsca. Podczas odzyskiwania granularnego tymczasowo potrzeba wolnego miejsca na poziomie 15% największej bazy danych Exchange.

** Jeśli system ESXi korzysta z pamięci masowej dołączonej do sieci SAN, zainstaluj agenta na komputerze podłączonym do tej samej sieci SAN. Agent będzie tworzył kopie zapasowe maszyn wirtualnych bezpośrednio z magazynu, a nie z hosta ESXi czy z sieci lokalnej. Szczegółowe instrukcje można znaleźć w sekcji "Agent dla VMware — tworzenie kopii zapasowych bez obciążania sieci lokalnej" (s. 735).

*** W przypadku środowiska Virtuozzo 7 obsługiwane są tylko kontenery ploop. Maszyny wirtualne nie są obsługiwane.

**** Maszyna wirtualna jest uznawana za wirtualną, jeśli jej kopie zapasowe są tworzone przez agenta zewnętrznego. Jeśli agent jest zainstalowany w systemie-gościu, operacje tworzenia kopii zapasowych i odzyskiwania są takie same jak w przypadku komputera fizycznego. Jeśli usługa Cyber Protection zidentyfikuje maszynę wirtualną za pomocą instrukcji CPUID, maszynie tej zostanie przypisany limit usługi dla maszyny wirtualnej. W przypadku korzystania z funkcji direct passthrough lub innej opcji maskującej identyfikator producenta procesora można przypisać tylko limity usług dla komputerów fizycznych.

Wymagania systemowe agentów

Agent	Miejsce na dysku wymagane do instalacji
Agent dla systemu Windows	1,2 GB
Agent dla systemu Linux	2 GB
Agent dla systemu Mac	1 GB
Agent dla SQL i agent dla systemu Windows	1,2 GB
Agent dla programu Exchange i agent dla systemu Windows	1,3 GB
Agent dla rozwiązania Data Loss Prevention	500 MB
Agent dla usługi Microsoft 365	500 MB
Agent dla usługi Active Directory i agent dla systemu Windows	2 GB

© Acronis International GmbH, 2003-2024

Agent dla VMware i agent dla systemu Windows	1,5 GB
Agent dla Hyper-V i agent dla systemu Windows	1,5 GB
Agent dla Virtuozzo i agent dla systemu Linux	1 GB
Agent dla Virtuozzo Hybrid Infrastructure	700 MB
Agent dla programu Oracle i agent dla systemu Windows	2,2 GB
Agent dla programu Oracle i agent dla systemu Linux	2 GB
Agent dla MySQL/MariaDB i agent dla systemu Linux	2 GB

Operacje dotyczące kopii zapasowych, w tym ich usuwanie, wymagają około 1 GB pamięci RAM na 1 TB kopii zapasowej. Szczytowe użycie pamięci może być różne, w zależności od ilości i typu danych przetwarzanych przez agenty.

Uwaga
W przypadku tworzenia kopii zapasowych w ramach bardzo dużych zestawów kopii zapasowych (o wielkości co najmniej 4 TB) zużycie pamięci RAM może wzrosnąć.

W systemach x64 operacje z nośnikiem startowym i odzyskiwanie dysku z ponownym uruchomieniem wymagają co najmniej 2 GB pamięci.

W przypadku obciążeń na nowoczesnych procesorach, takich jak Intel Core 11. generacji lub AMD Ryzen 7 z obsługą technologii CET, niektóre funkcje usługi Agent dla funkcji Zapobieganie utracie danych są wyłączone w celu uniknięcia konfliktów. W poniższej tabeli pokazana jest dostępność funkcji Kontrola urządzeń i Advanced DLP w systemach z takimi procesorami.

Funkcje	Kontrola urządzeń	Advanced DLP
Kanały lokalne		
Magazyn wymienny	n/d	Tak
Zaszyfrowany magazyn wymienny	Tak	n/d
Drukarki	n/d	Nie
Przekierowane zamapowane dyski	n/d	Tak
Przekierowane dane schowka	n/d	Nie
Komunikacja sieciowa		
E-mail SMTP	n/d	Tak
Microsoft Outlook (MAPI)	n/d	Tak
Notatki IBM	n/d	Nie

© Acronis International GmbH, 2003-2024

Aplikacje Webmail	n/d	Tak
Wiadomości błyskawiczne (ICQ)	n/d	Nie
Wiadomości błyskawiczne (Viber)	n/d	Nie
Wiadomości błyskawiczne (IRC, Jabber, Skype, Viber)	n/d	Tak
Usługi udostępniania plików	n/d	Tak
Portale społecznościowe	n/d	Tak
Udostępnianie plików w sieci lokalnej (SMB)	n/d	Tak
Dostęp do Internetu (HTTP/HTTPS)	n/d	Tak
Przesyłanie plików (FTP/FTPS)	n/d	Tak
Dopuszczanie transferu danych		
Zarządzanie listą dozwolonych typów urządzeń	n/d	Tak
Zezwalanie na komunikację sieciową	n/d	Tak
Lista dozwolonych hostów zdalnych	n/d	Tak
Lista dozwolonych aplikacji	n/d	Tak
Urządzenia peryferyjne		
Magazyn wymienny	Tak	Tak
Zaszyfrowany magazyn wymienny	Tak	Tak
Drukarki	Nie	Nie
Urządzenia mobilne połączone przy użyciu protokołu MTP	Nie	Nie
Adaptery Bluetooth	Tak	Tak
Dyski optyczne	Tak	Tak
Dyskietki	Tak	Tak
Schowek systemu Windows	Nie	Nie
Rejestrowanie zrzutu ekranu	Nie	Nie
Przekierowane zamapowane dyski	Tak	Tak
Przekierowane dane schowka	Nie	Nie
Ochrona własna w narzędziu Cyber Protect Agent		
Ochrona przez zwykłych użytkowników końcowych	Tak	Tak
Ochrona przez lokalnych administratorów systemu	Tak	Tak

© Acronis International GmbH, 2003-2024

Pobieranie agentów ochrony

Przed zainstalowaniem agenta należy pobrać jego plik instalacyjny z konsoli Cyber Protect.

Aby pobrać agenta podczas dodawania obciążenia do ochrony

1. W konsoli usługi Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. W prawym górnym rogu kliknij **Dodaj urządzenie**.
3. W panelu **Dodaj urządzenia** wybierz wersję agenta w menu rozwijanym **Kanał wersji**.
   - **Poprzednia wersja** — pobierz agenta z poprzedniej wersji.
   - **Bieżąca** — pobierz najnowszą dostępną wersję agenta.
4. Wybierz agenta odpowiadającego systemowi operacyjnemu dodawanego obciążenia.
   Zostanie otwarte okno dialogowe **Zapisz jako**.
5. [Tylko w przypadku komputerów Mac z procesorami Apple Silicon (takimi jak Apple M1)] Kliknij **Anuluj**. W nowo otwartym panelu **Dodaj komputer Mac** kliknij łącze **Pobierz instalator ARM**.
6. Wybierz lokalizację, w której chcesz zapisać plik instalacyjny agenta, i kliknij **Zapisz**.

Aby pobrać agenta do późniejszego użycia

1. W prawym górnym rogu konsoli usługi Cyber Protect kliknij ikonę **Użytkownik**.
2. Kliknij **Do pobrania**.
3. W oknie dialogowym **Do pobrania** wybierz wersję agenta w menu rozwijanym **Kanał wersji**.
   - **Poprzednia wersja** — pobierz agenta z poprzedniej wersji.
   - **Bieżąca** — pobierz najnowszą dostępną wersję agenta.
4. Przewiń listę dostępnych instalatorów, aby znaleźć potrzebny instalator agenta, a następnie kliknij ikonę pobierania znajdującą się na końcu jego wiersza.
   Zostanie otwarte okno dialogowe **Zapisz jako**.
5. Wybierz lokalizację, w której chcesz zapisać plik instalacyjny agenta, i kliknij **Zapisz**.

Pakiety systemu Linux

Aby dodać potrzebne moduły do jądra systemu Linux, program instalacyjny wymaga następujących pakietów systemu Linux:

- Pakiet z nagłówkami lub źródłami jądra. Wersja pakietu musi odpowiadać wersji jądra.
- System kompilatora GNU Compiler Collection (GCC). Wersja kompilatora GCC musi być taka sama jak ta, przy użyciu której skompilowano jądro.
- Narzędzie Make.
- Interpreter języka Perl.
- Biblioteki `libelf-dev`, `libelf-devel` lub `elfutils-libelf-devel` do budowy jąder od 4.15 i konfigurowanych za pomocą polecenia CONFIG_UNWINDER_ORC=y. W niektórych dystrybucjach, takich jak Fedora 28, konieczna jest instalacja odrębna z nagłówków jądra.

© Acronis International GmbH, 2003-2024

Nazwy tych pakietów mogą się różnić w zależności od dystrybucji systemu Linux.

W systemach Red Hat Enterprise Linux, CentOS i Fedora pakiety te są normalnie instalowane przez program instalacyjny. W pozostałych dystrybucjach pakiety te należy zainstalować, jeśli nie są jeszcze zainstalowane lub nie występują w wymaganych wersjach.

Czy wymagane pakiety są już zainstalowane?

Aby sprawdzić, czy pakiety są już zainstalowane, wykonaj następujące czynności:

1. Uruchom następujące polecenie, aby poznać wersję jądra i wymaganą wersję kompilatora GCC:

   ```
   cat /proc/version
   ```

   Wynikiem działania tego polecenia są wiersze podobne do następujących: `Linux version 2.6.35.6` i `gcc version 4.5.1`
2. Uruchom następujące polecenie, aby sprawdzić, czy jest zainstalowane narzędzie Make i kompilator GCC:

   ```
   make -v
   gcc -v
   ```

   W przypadku kompilatora **gcc** sprawdź, czy wersja zwrócona przez polecenie jest taka sama jak `gcc version` w kroku 1. W przypadku narzędzia **make** wystarczy sprawdzić, czy polecenie uruchamia się.
3. Sprawdź, czy jest zainstalowana odpowiednia wersja pakietów do kompilowania modułów jądra:
   - W systemach Red Hat Enterprise Linux, CentOS i Fedora uruchom następujące polecenie:

     ```
     yum list installed | grep kernel-devel
     ```

   - W systemie Ubuntu uruchom następujące polecenia:

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   W obu przypadkach sprawdź, czy wersje pakietów są takie same jak wersja `Linux version` w kroku 1.
4. Uruchom następujące polecenie, aby sprawdzić, czy jest zainstalowany interpreter języka Perl:

   ```
   perl --version
   ```

   Jeśli zostanie wyświetlona informacja o wersji języka Perl, interpreter jest zainstalowany.
5. W systemach Red Hat Enterprise Linux, CentOS i Fedora uruchom następujące polecenie celem sprawdzenia, czy zainstalowano pakiet `elfutils-libelf-devel`:

   ```
   yum list installed | grep elfutils-libelf-devel
   ```


© Acronis International GmbH, 2003-2024

Jeśli zostanie wyświetlona informacja o wersji biblioteki, oznacza to, że biblioteka jest zainstalowana.

Instalowanie pakietów z repozytorium

Poniższa tabela przedstawia sposoby instalacji wymaganych pakietów w różnych dystrybucjach systemu Linux.

Dystrybucja systemu Linux	Nazwy pakietów	Sposób instalacji
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Program instalacyjny automatycznie pobierze i zainstaluje pakiety z użyciem subskrypcji Red Hat.
	perl	Uruchom następujące polecenie: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Program instalacyjny automatycznie pobierze i zainstaluje pakiety.
	perl	Uruchom następujące polecenie: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Uruchom następujące polecenia:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source
	gcc
	make
	perl
		`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

Pakiety zostaną pobrane z repozytorium dystrybucji i zainstalowane.

W przypadku innych dystrybucji systemu Linux dokładne nazwy wymaganych pakietów i metody ich instalacji można znaleźć w dokumentacji dystrybucji.

© Acronis International GmbH, 2003-2024

Ręczne instalowanie pakietów

Ręczna instalacja pakietów może być konieczna w następujących przypadkach:

- Komputer nie ma aktywnej subskrypcji Red Hat lub połączenia z Internetem.
- Program instalacyjny nie może znaleźć wersji pakietów **kernel-devel** lub **gcc** odpowiadających wersji jądra. Jeśli dostępny pakiet **kernel-devel** jest nowszy niż jądro, należy ręcznie zaktualizować jądro lub zainstalować odpowiednią wersję pakietu **kernel-devel**.
- Użytkownik ma wymagane pakiety w sieci lokalnej i nie chce tracić czasu na ich automatyczne wyszukiwanie i pobieranie.

Uzyskaj pakiety z sieci lokalnej lub z witryny internetowej zaufanej innej firmy i zainstaluj je zgodnie z poniższymi wskazówkami:

- W systemie Red Hat Enterprise Linux, CentOS lub Fedora uruchom jako użytkownik root następujące polecenie:

  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

- W systemie Ubuntu uruchom następujące polecenie:

  ```
  sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

Przykład: ręczne instalowanie pakietów w systemie Fedora 14

Wykonaj następujące czynności, aby zainstalować wymagane pakiety w systemie Fedora 14 na komputerze 32-bitowym:

1. Uruchom następujące polecenie, aby określić wersję jądra i wymaganą wersję kompilatora GCC:

   ```
   cat /proc/version
   ```

   W wyniku jego uruchomienia zostają zwrócone następujące informacje:

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. Uzyskaj pakiety **kernel-devel** i **gcc** odpowiadające tej wersji jądra:

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Uzyskaj pakiet **make** dla systemu Fedora 14:

   ```
   make-3.82-3.fc14.i686
   ```

4. Zainstaluj pakiety, uruchamiając jako użytkownik root następujące polecenie:

© Acronis International GmbH, 2003-2024

```
rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
rpm -ivh gcc-4.5.1.fc14.i686.rpm
rpm -ivh make-3.82-3.fc14.i686
```

Wszystkie wspomniane pakiety można wskazać w jednym poleceniu `rpm`. Zainstalowanie każdego z pakietów może wymagać instalacji dodatkowych pakietów wynikających z określonych zależności.

Konfigurowanie ustawień serwera proxy

Agenty ochrony mogą przesyłać dane przez serwer proxy HTTP/HTTPS. Serwer musi działać przez tunel HTTP bez skanowania ruchu HTTP lub ingerowania w niego. Serwery proxy działające w trybie MITM (man-in-the-middle) nie są obsługiwane.

Ponieważ agent podczas instalacji rejestruje się w chmurze, to podczas instalacji agenta lub wcześniej trzeba skonfigurować ustawienia serwera proxy.

W przypadku systemu Windows

Jeśli w systemie jest już skonfigurowany serwer proxy w sekcji **Panel sterowania** > **Opcje internetowe** > **Połączenia**, program instalacyjny automatycznie odczyta ustawienia serwera proxy z rejestru i ich użyje.

Użyj tej procedury, jeśli chcesz wykonać następujące zadania.

- Skonfigurowanie ustawień serwera proxy przed instalacją agenta.
- Zaktualizowanie ustawień serwera proxy po instalacji agenta.

Aby skonfigurować ustawienia serwera proxy podczas instalacji agenta, zobacz "Instalowanie agentów ochrony w systemie Windows" (s. 84).

Uwaga
Ta procedura dotyczy tylko sytuacji, gdy na komputerze nie ma pliku `http-proxy.yaml`. Jeśli na komputerze jest plik `http-proxy.yaml`, trzeba będzie zaktualizować ustawienia serwera proxy w tym pliku, ponieważ zastępują one ustawienia zawarte w pliku `aakore.yaml`.

Jeśli skonfigurujesz ustawienia serwera proxy przy użyciu narzędzia Cyber Protection Monitor, zostanie utworzony plik `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml`. Aby uzyskać więcej informacji, zobacz "Konfigurowanie ustawień serwera proxy w narzędziu Cyber Protect Monitor" (s. 307).

Aby otworzyć plik `http-proxy.yaml`, musisz należeć do grupy Administratorzy w systemie Windows.

Aby skonfigurować ustawienia serwera proxy

1. Utwórz nowy dokument tekstowy i otwórz go w edytorze tekstów, np. w programie Notatnik.
2. Skopiuj i wklej do pliku poniższe wiersze.

© Acronis International GmbH, 2003-2024

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Zastąp `proxy.company.com` nazwą hosta / adresem IP serwera proxy, a `000001bb` — wartością szesnastkową numeru portu. Na przykład wartość `000001bb` oznacza port 443.
4. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `proxy_login` i `proxy_password` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.
5. Zapisz dokument pod nazwą `proxy.reg`.
6. Uruchom plik jako administrator.
7. Potwierdź, że chcesz edytować rejestr systemu Windows.
8. Jeśli agent nie jest jeszcze zainstalowany na obciążeniu, możesz go teraz zainstalować. Jeśli agent jest już zainstalowany na obciążeniu, przejdź do następnego kroku.
9. Otwórz plik `%programdata%\Acronis\Agent\etc\aakore.yaml` w edytorze tekstów.
   Aby otworzyć ten plik, musisz należeć do grupy Administratorzy w systemie Windows.
10. Znajdź sekcję **env** lub ją utwórz i dodaj następujące wiersze.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. Zastąp zmienne `proxy_login` i `proxy_password` poświadczeniami dostępu do serwera proxy, a zmienną `proxy_address:port` — adresem i numerem portu serwera proxy.
12. W menu **Start** kliknij **Uruchom**, a następnie wpisz: **cmd** i kliknij **OK**.
13. Uruchom ponownie usługę aakore za pomocą następujących poleceń.

```
net stop aakore
net start aakore
```

14. Uruchom ponownie agenta za pomocą następujących poleceń.

```
net stop mms
net start mms
```

W przypadku systemu macOS

Użyj tej procedury, jeśli chcesz wykonać następujące zadania.

- Skonfigurowanie ustawień serwera proxy przed instalacją agenta.
- Zaktualizowanie ustawień serwera proxy po instalacji agenta.

© Acronis International GmbH, 2003-2024

Aby skonfigurować ustawienia serwera proxy podczas instalacji agenta, zobacz "Instalowanie agentów ochrony w systemie macOS" (s. 89).

Aby skonfigurować ustawienia serwera proxy

1. Utwórz plik `/Library/Application Support/Acronis/Registry/Global.config` i otwórz go w edytorze tekstów, np. w programie Text Edit.
2. Skopiuj i wklej do pliku poniższe wiersze.

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. Zastąp `proxy.company.com` nazwą hosta / adresem IP serwera proxy, a `443` — wartością dziesiętną numeru portu.
4. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `proxy_login` i `proxy_password` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.
5. Zapisz plik.
6. Jeśli agent nie jest jeszcze zainstalowany na obciążeniu, możesz go teraz zainstalować. Jeśli agent jest już zainstalowany na obciążeniu, przejdź do następnego kroku.
7. Otwórz plik `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` w edytorze tekstów.
8. Znajdź sekcję **env** lub ją utwórz i dodaj następujące wiersze.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

9. Zastąp zmienne `proxy_login` i `proxy_password` poświadczeniami dostępu do serwera proxy, a zmienną `proxy_address:port` — adresem i numerem portu serwera proxy.
10. Przejdź do **Aplikacje** > **Narzędzia** > **Terminal**.
11. Uruchom ponownie usługę aakore za pomocą następujących poleceń.

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. Uruchom ponownie agenta za pomocą następujących poleceń.

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

W przypadku systemu Linux

© Acronis International GmbH, 2003-2024

Uruchom plik instalacyjny z następującymi parametrami: `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD`. Poniższa procedura umożliwia zaktualizowanie ustawień serwera proxy po zainstalowaniu agenta ochrony.

Aby skonfigurować ustawienia serwera proxy

1. Otwórz plik `/etc/Acronis/Global.config` w edytorze tekstów.
2. Wykonaj jedną z następujących czynności:
   - Jeśli ustawienia serwera proxy zostały określone podczas instalacji agenta, znajdź następującą sekcję:

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - Jeśli ustawienia serwera proxy nie zostały określone podczas instalacji agenta, skopiuj poniższe wiersze i wklej je do pliku między znacznikami `<registry name="Global">...</registry>`.

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

3. Zastąp wartość `ADDRESS` nową nazwą hosta / adresem IP serwera proxy, a wartość `PORT` — wartością dziesiętną numeru portu.
4. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `LOGIN` i `PASSWORD` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.
5. Zapisz plik.
6. Otwórz plik `/opt/acronis/etc/aakore.yaml` w edytorze tekstów.
7. Znajdź sekcję **env** lub ją utwórz i dodaj następujące wiersze:

   ```
   env:
       http-proxy: proxy_login:proxy_password@proxy_address:port
       https-proxy: proxy_login:proxy_password@proxy_address:port
   ```

8. Zastąp zmienne `proxy_login` i `proxy_password` poświadczeniami dostępu do serwera proxy, a zmienną `proxy_address:port` — adresem i numerem portu serwera proxy.
9. Uruchom ponownie usługę aakore za pomocą następującego polecenia.

   ```
   sudo service aakore restart
   ```


© Acronis International GmbH, 2003-2024

10. W przeciwnym wypadku uruchom ponownie agenta, wykonując w dowolnym katalogu następujące polecenie.

```
sudo service acronis_mms restart
```

W przypadku nośnika startowego

Podczas pracy z nośnikiem startowym może wystąpić konieczność uzyskania dostępu do chmury za pośrednictwem serwera proxy. Aby skonfigurować ustawienia serwera proxy, kliknij **Narzędzia** > **Serwer proxy**, a następnie skonfiguruj nazwę hosta / adres IP, port i poświadczenia serwera proxy.

Dynamiczna instalacja i dezinstalacja komponentów

W przypadku obciążeń z systemem Windows chronionych przez agenta w wersji 15.0.26986 (wydanej w maju 2021 r.) lub nowszej niektóre komponenty są instalowane dynamicznie, czyli tylko wtedy, gdy wymaga tego plan ochrony. Są to:

- Agent dla usługi Filtrowanie adresów URL — wymagany do działania funkcji usługi Filtrowanie adresów URL.
- Agent dla funkcji Ochrona przed złośliwym oprogramowaniem — wymagany do działania funkcji ochrony przed złośliwym oprogramowaniem.
- Agent dla funkcji Zapobieganie utracie danych — wymagany do działania funkcji kontroli urządzeń.

Domyślnie te komponenty nie są instalowane. Odpowiedni komponent zostanie zainstalowany automatycznie w przypadku objęcia obciążenia ochroną przez plan, w którym jest włączony którykolwiek z poniższych modułów:

- Ochrona przed wirusami i złośliwym oprogramowaniem
- Filtrowanie adresów URL
- Kontrola urządzeń

I analogicznie: jeśli żaden plan ochrony nie wymaga już funkcji ochrony przed złośliwym oprogramowaniem, filtrowania adresów URL ani kontroli urządzeń, odpowiedni komponent zostanie automatycznie odinstalowany.

Dynamiczna instalacja lub dezinstalacja komponentów następuje w ciągu 10 minut od zmiany planu ochrony. Jeśli jednak jest wykonywana którakolwiek z poniższych operacji, dynamiczna instalacja lub dezinstalacja rozpocznie się zaraz po zakończeniu tej operacji:

- Kopia zapasowa
- Odzyskiwanie
- Replikacja kopii zapasowej
- Replikacja maszyn wirtualnych
- Testowanie repliki
- Uruchamianie maszyny wirtualnej z kopii zapasowej (łącznie z finalizacją)

© Acronis International GmbH, 2003-2024

- Przełączanie awaryjne w ramach odzyskiwania po awarii
- Powrót po awarii w ramach odzyskiwania po awarii
- Uruchamianie skryptu (w przypadku funkcji Obsługa skryptów cybernetycznych)
- Instalacja poprawek
- Kopia zapasowa konfiguracji hosta ESXi

Przyznawanie wymaganych uprawnień systemowych modułowi Agent rozwiązania Connect

Aby włączyć wszystkie funkcje pulpitu zdalnego na obciążeniach z systemem macOS, oprócz uprawnienia dostępu do całego dysku należy przyznać modułowi Agent rozwiązania Connect następujące uprawnienia:

- Nagrywanie ekranu — umożliwia nagrywanie ekranu na obciążeniu z systemem macOS przy użyciu protokołu NEAR. Dopóki to uprawnienie nie zostanie przyznane, wszystkie połączenia zdalnego sterowania będą odrzucane.
- Dostępność — umożliwia włączenie połączeń zdalnych w trybie sterowania przy użyciu protokołu NEAR.
- Mikrofon — umożliwia przekierowanie dźwięku z obciążenia zdalnego z systemem macOS do obciążenia lokalnego przy użyciu protokołu NEAR. Aby włączyć funkcję przekierowania dźwięku, na obciążeniu musi być zainstalowany sterownik przechwytywania dźwięku. Aby uzyskać więcej informacji, zobacz "Przekierowanie dźwięku w ramach połączenia zdalnego" (s. 1080).
- Automatyzacja — umożliwia czynność opróżniania kosza.

Po uruchomieniu agenta na obciążeniu z systemem macOS sprawdzi on, czy agent ma te prawa, i w razie potrzeby poprosi o przyznanie odpowiednich uprawnień.

Aby przyznać uprawnienie Nagrywanie ekranu

1. W oknie dialogowym **Przyznaj wymagane uprawnienia systemowe** dla agenta Cyber Protect kliknij **Skonfiguruj uprawnienia systemowe**.
2. W oknie dialogowym **Uprawnienia systemowe** kliknij **Poproś o uprawnienie Nagrywanie ekranu**.
3. Kliknij **Otwórz preferencje systemowe**.
4. Wybierz **Agent rozwiązania Connect**.

Jeśli agent nie ma tego uprawnienia, gdy próbujesz uzyskać dostęp zdalny do obciążenia, wyświetli okno dialogowe Prośba o uprawnienie Nagrywanie ekranu. Tylko lokalny użytkownik może odpowiedzieć na monit przedstawiony w tym oknie dialogowym.

Aby przyznać uprawnienie Dostępność

1. W oknie dialogowym **Przyznaj wymagane uprawnienia systemowe** dla agenta Cyber Protect kliknij **Skonfiguruj uprawnienia systemowe**.

© Acronis International GmbH, 2003-2024

2. W oknie dialogowym **Uprawnienia systemowe** kliknij **Poproś o uprawnienie Dostępność**.
3. Kliknij **Otwórz preferencje systemowe**.
4. Kliknij ikonę kłódki w lewym dolnym rogu okna, aby została zastąpiona ikoną otwartej kłódki. System poprosi o podanie hasła administratora w celu dokonania zmian.
5. Wybierz **Agent rozwiązania Connect**.

Aby przyznać uprawnienie Mikrofon

1. W obszarze **Przyznaj wymagane uprawnienia systemowe** w oknie dialogowym modułu Agent rozwiązania Connect kliknij **Skonfiguruj uprawnienia systemowe**.
2. W oknie dialogowym **Uprawnienia systemowe** kliknij **Poproś o uprawnienie Mikrofon**.
3. Kliknij **OK**.

Uwaga
Musisz też zainstalować sterownik przechwytywania dźwięku na obciążeniu z systemem macOS, aby agent mógł skorzystać z przyznanego uprawnienia i przekierować dźwięk obciążenia. Aby uzyskać więcej informacji, zobacz "Przekierowanie dźwięku w ramach połączenia zdalnego" (s. 1080).

Aby przyznać uprawnienie Automatyzacja

1. W obszarze **Przyznaj wymagane uprawnienia systemowe** w oknie dialogowym modułu Agent rozwiązania Connect kliknij **Skonfiguruj uprawnienia systemowe**.
2. W oknie dialogowym **Uprawnienia systemowe** kliknij **Poproś o uprawnienie Automatyzacja**.

Instalowanie agentów ochrony przy użyciu graficznego interfejsu użytkownika

Instalowanie agentów ochrony w systemie Windows

Wymagania wstępne

Pobierz potrzebnego agenta na obciążenie, które planujesz chronić. Zobacz "Pobieranie agentów ochrony" (s. 74).

Aby zainstalować agenta dla systemu Windows

1. Upewnij się, że komputer ma połączenie z Internetem.
2. Zaloguj się jako administrator i uruchom instalator.
3. [Opcjonalnie] Kliknij **Dostosuj ustawienia instalacji** i wprowadź odpowiednie zmiany, jeśli chcesz:
   - Zmienić komponenty do zainstalowania (na przykład wyłączyć instalację narzędzia Cyber Protection Monitor lub narzędzia wiersza polecenia albo zainstalować agenta dla usługi Ochrona przed złośliwym oprogramowaniem lub agenta dla usługi Filtrowanie adresów URL).

© Acronis International GmbH, 2003-2024

Uwaga
Na komputerach z systemem Windows funkcja ochrony przed złośliwym oprogramowaniem wymaga instalacji agenta dla usługi Ochrona przed złośliwym oprogramowaniem, a funkcja filtrowania adresów URL wymaga instalacji agenta dla usługi Filtrowanie adresów URL. Agenty te są instalowane automatycznie w przypadku chronionych maszyn, jeśli w ich planach ochrony włączono moduł **Ochrona przed wirusami i złośliwym oprogramowaniem** i/lub **Filtrowanie adresów URL**.

- Zmienić metodę rejestracji obciążenia w usłudze Cyber Protection. Możesz przełączyć z opcji **Użyj konsoli usługi** (opcja domyślna) na opcję **Użyj poświadczeń** lub **Użyj tokenu rejestracji**.
- Zmienić ścieżkę instalacji.
- Zmienić konto użytkownika, na którym będzie działać usługa agenta. Szczegółowe informacje można znaleźć w artykule "Zmienianie konta logowania na komputerach z systemem Windows" (s. 86).
- Aby zweryfikować lub zmienić nazwę hosta / adres IP, port i poświadczenia serwera proxy. W przypadku włączenia serwera proxy w systemie Windows zostanie on automatycznie wykryty i użyty.

4. Kliknij **Zainstaluj**.
5. [Tylko w przypadku instalowania agenta dla VMware] Podaj adres i poświadczenia dostępu serwera vCenter lub autonomicznego hosta ESXi, na którym chcesz tworzyć kopie zapasowe maszyn wirtualnych i je odzyskiwać, a następnie kliknij **Gotowe**.
   W celu uzyskania dostępu do serwera vCenter lub hosta ESXi warto korzystać ze specjalnego konta, a nie z już istniejącego konta z rolą Administrator. Dodatkowe informacje można znaleźć w sekcji "Wymagane uprawnienia dla agenta dla VMware" (s. 744).
6. [Tylko w przypadku instalowania na kontrolerze domeny] Określ konto użytkownika, które będzie służyć do uruchamiania usługi agenta, a następnie kliknij **Gotowe**. Ze względów bezpieczeństwa program instalacyjny nie tworzy automatycznie nowych kont na kontrolerze domeny.

   Uwaga
   Wskazane konto użytkownika musi mieć przyznane prawo `Logowanie jako usługa`. Konto to musi już być używane na kontrolerze domeny, aby jego folder profilu został utworzony na tym komputerze.

   Dodatkowe informacje o instalowaniu agenta na kontrolerze domeny w trybie tylko do odczytu można znaleźć w tym artykule z bazy wiedzy Knowledge Base.
7. Jeśli w kroku 3 została zachowana domyślna metoda rejestracji **Użyj konsoli usługi**, poczekaj, aż pojawi się ekran rejestracji, a następnie przejdź do następnego kroku. W przeciwnym razie nie trzeba wykonywać żadnych innych czynności.

© Acronis International GmbH, 2003-2024

8. Zarejestruj agenta na koncie dzierżawcy-klienta. Więcej informacji na temat rejestracji można znaleźć w sekcji "Rejestrowanie maszyn przy użyciu graficznego interfejsu użytkownika" (s. 127).
9. [Jeśli agent jest zarejestrowany na koncie, którego dzierżawca jest w trybie zgodności] Ustaw hasło szyfrowania.

Zmienianie konta logowania na komputerach z systemem Windows

Na ekranie **Wybierz komponenty** wskaż konto, na którym będą działać usługi, w polu **Konto logowania dla usługi agenta**. Można wybrać jedną z następujących opcji:

- **Użyj kont użytkowników usługi** (domyślne w przypadku usługi agenta)
  Konta użytkowników usługi to konta w systemie Windows używane do uruchamiania usług. Ustawienie to ma tę zaletę, że zasady zabezpieczeń domeny nie wpływają na prawa użytkowników tych kont. Domyślnie agent działa na koncie **System lokalny**.
- **Utwórz nowe konto**
  Nazwą konta dla danego agenta będzie Agent User.
- **Użyj następującego konta**
  Jeśli agent zostanie zainstalowany na kontrolerze domeny, system wyświetli monit o określenie istniejących już kont (lub tego samego konta) na potrzeby agenta. Ze względów bezpieczeństwa system nie tworzy automatycznie nowych kont na kontrolerze domeny.
  Konto użytkownika określone podczas uruchamiania programu instalacyjnego na kontrolerze domeny musi mieć przyznane prawo `Logowanie jako usługa`. Konto to musi już być używane na kontrolerze domeny, aby jego folder profilu został utworzony na tym komputerze.
  Dodatkowe informacje o instalowaniu agenta na kontrolerze domeny w trybie tylko do odczytu można znaleźć w tym artykule z bazy wiedzy Knowledge Base.

W przypadku wybrania opcji **Utwórz nowe konto** lub **Użyj następującego konta** dopilnuj, aby zasady zabezpieczeń domeny nie wpływały na prawa powiązanych kont. Jeśli konto straci prawa użytkownika przypisane podczas instalacji, komponent może działać niepoprawnie lub wcale nie działać.

Uprawnienia wymagane w przypadku konta logowania

Agent ochrony jest uruchamiany jako usługa Managed Machine Service (MMS) na komputerze z systemem Windows. Aby agent działał jak należy, konto, na którym zostanie uruchomiony, musi mieć określone prawa. Dlatego też użytkownikowi usługi MMS należy przyznać następujące uprawnienia:

1. Przynależność do grup **Operatorzy kopii zapasowych** i **Administratorzy**. W przypadku kontrolera domeny użytkownik musi należeć do grupy **Administratorzy domeny**.
2. Uprawnienie **Pełna kontrola** do folderu `%PROGRAMDATA%\Acronis` (w systemach Windows XP i Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) i do podfolderów.
3. Uprawnienie **Pełna kontrola** do pewnych kluczy rejestru w kluczu: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Przyznane następujące prawa użytkownika:

© Acronis International GmbH, 2003-2024

- Zaloguj jako usługa
- Dostosuj przydziały pamięci dla procesu
- Zamień token na poziomie procesu
- Modyfikuj wartości środowiskowe oprogramowania układowego

Jak przypisać prawa użytkownika

Aby przypisać prawa użytkownika, należy postąpić zgodnie z poniższymi instrukcjami (w przykładzie posłużono się prawem użytkownika **Logowanie w trybie usługi**, ale instrukcje są takie same w przypadku wszystkich praw):

1. Zaloguj się do komputera przy użyciu konta z uprawnieniami administracyjnymi.
2. Otwórz **Narzędzia administracyjne** w **Panelu sterowania** (lub naciśnij Win+R, wpisz **control admintools** i naciśnij Enter) i otwórz **Zasady zabezpieczeń lokalnych**.
3. Rozwiń gałąź **Zasady lokalne** i kliknij **Przypisywanie praw użytkownika**.
4. W prawym okienku kliknij prawym przyciskiem myszy **Logowanie w trybie usługi** i wybierz **Właściwości**.
5. Kliknij przycisk **Dodaj użytkownika lub grupę**, aby dodać nowego użytkownika.
6. W oknie **Wybierz użytkowników, komputery, konta usług lub grupy** znajdź właściwego użytkownika i kliknij **OK**.
7. Kliknij **OK** w obszarze **Logowanie w trybie usługi — właściwości**, aby zapisać zmiany.

Ważne
Dopilnuj, aby użytkownik, któremu przyznano prawo **Logowanie w trybie usługi**, nie znajdował się na liście zasad **Odmowa logowania w trybie usługi** w sekcji **Zasady zabezpieczeń lokalnych**.

Uwaga: lepiej nie zmieniać ręcznie kont logowania po zakończeniu instalacji.

Instalowanie agentów ochrony w systemie Linux

Przygotowanie

- Pobierz potrzebnego agenta na komputer, który planujesz chronić. Zobacz "Pobieranie agentów ochrony" (s. 74).
- Upewnij się, że na komputerze są zainstalowane niezbędne pakiety systemu Linux.
- Instalując agenta w systemie SUSE Linux, koniecznie użyj polecenia `su -`, a nie `sudo`. Jeśli tego nie zrobisz, to przy próbie rejestracji agenta za pośrednictwem konsoli Cyber Protect wystąpi następujący błąd: `Nie udało się uruchomić przeglądarki internetowej. Brak dostępnego ekranu.`

  Niektóre dystrybucje systemu Linux, na przykład SUSE, nie analizują zmiennej DISPLAY w przypadku użycia polecenia sudo i instalator nie może otworzyć przeglądarki w graficznym interfejsie użytkownika (GUI).

© Acronis International GmbH, 2003-2024

Instalacja

Aby zainstalować agenta dla systemu Linux, potrzebujesz co najmniej 2 GB wolnego miejsca na dysku.

Aby zainstalować agenta dla systemu Linux

1. Upewnij się, że komputer ma połączenie z Internetem.
2. Jako użytkownik root przejdź do katalogu z plikiem instalacyjnym, zmień plik w plik wykonywalny, a następnie go uruchom.

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

   Jeśli w sieci jest włączony serwer proxy, podczas uruchamiania pliku instalacyjnego należy podać nazwę hosta / adres IP oraz port tego serwera w następującym formacie: `--http-proxy-host=ADDRESS` `--http-proxy-port=PORT` `--http-proxy-login=LOGIN` `--http-proxy-password=PASSWORD`.

   Jeśli chcesz zmienić domyślną metodę rejestracji komputera w usłudze Cyber Protection, uruchom plik instalacyjny przy użyciu jednego z poniższych parametrów:

   - `--register-with-credentials` — powoduje wyświetlenie monitu o nazwę użytkownika i hasło podczas instalacji
   - `--token=STRING` – umożliwia wymuszenie użycia tokenu rejestracji
   - `--skip-registration` — umożliwia pominięcie rejestracji
3. Zaznacz pola wyboru odpowiadające agentom, które chcesz zainstalować. Dostępne są następujące agenty:
   - Agent dla systemu Linux
   - Agent dla Virtuozzo
   - Agent dla programu Oracle
   - Agent dla MySQL/MariaDB

   Agent dla Virtuozzo, agent dla programu Oracle i agent dla MySQL/MariaDB wymagają zainstalowania również agenta dla systemu Linux (64-bitowego).
4. W przypadku zachowania w kroku 2 domyślnej metody rejestracji, przejdź do następnego kroku. W przeciwnym razie wprowadź nazwę użytkownika i hasło do usługi Cyber Protection lub poczekaj, aż komputer zostanie zarejestrowany za pomocą tokenu.
5. Zarejestruj agenta na koncie dzierżawcy-klienta. Więcej informacji na temat rejestracji można znaleźć w sekcji "Rejestrowanie maszyn przy użyciu graficznego interfejsu użytkownika" (s. 127).
6. [Jeśli agent jest zarejestrowany na koncie, którego dzierżawca jest w trybie zgodności] Ustaw hasło szyfrowania.
7. Jeśli na komputerze jest włączona funkcja UEFI Secure Boot, pojawi się informacja o konieczności ponownego uruchomienia systemu po zakończeniu instalacji. Koniecznie zapamiętaj, jakiego

© Acronis International GmbH, 2003-2024

hasła (hasła użytkownika root czy hasła „acronis”) należy użyć.

Uwaga
Instalacja wygeneruje nowy klucz, który służy do podpisywania modułów jądra. Musisz zarejestrować ten nowy klucz na liście kluczy właściciela komputera przez ponowne uruchomienie komputera. Bez rejestracji nowego klucza agent nie będzie działać. Jeśli po instalacji agenta zostanie włączona funkcja UEFI Secure Boot, trzeba ponownie zainstalować agenta.

8. Po instalacji wykonaj jedną z następujących czynności:
   - Jeśli w ramach poprzedniego kroku pojawił się monit o ponowne uruchomienie systemu, kliknij **Uruchom ponownie**.

     Podczas ponownego uruchamiania systemu wybierz opcję zarządzania kluczem właściciela komputera, zaznacz **Zarejestruj klucz właściciela komputera**, a następnie zarejestruj klucz przy użyciu hasła zalecanego w poprzednim kroku.
   - W przeciwnym razie kliknij **Zakończ**.

Informacje dotyczące rozwiązywania problemów są dostępne w pliku:
`/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

Instalowanie agentów ochrony w systemie macOS

Wymagania wstępne

Pobierz potrzebnego agenta na obciążenie, które planujesz chronić. Zobacz "Pobieranie agentów ochrony" (s. 74).

Aby zainstalować agenta dla systemu Mac (x64 lub ARM64)

1. Upewnij się, że komputer ma połączenie z Internetem.
2. Kliknij dwukrotnie plik instalacyjny (.dmg).
3. Poczekaj, aż system operacyjny zamontuje instalacyjny obraz dysku.
4. Kliknij dwukrotnie **Zainstaluj**.
5. Jeśli w danej sieci jest włączony serwer proxy, kliknij **Agent ochrony** na pasku menu, kliknij **Ustawienia serwera proxy**, a następnie podaj nazwę hosta lub adres IP serwera proxy, jego port oraz odpowiednie poświadczenia dostępu.
6. Jeśli pojawi się monit, podaj poświadczenia administratora.
7. Kliknij **Kontynuuj**.
8. Poczekaj, aż pojawi się ekran rejestracji.
9. Zarejestruj agenta na koncie dzierżawcy-klienta. Więcej informacji na temat rejestracji można znaleźć w sekcji "Rejestrowanie maszyn przy użyciu graficznego interfejsu użytkownika" (s. 127).
10. [Jeśli agent jest zarejestrowany na koncie, którego dzierżawca jest w trybie zgodności] Ustaw hasło szyfrowania.

© Acronis International GmbH, 2003-2024

11. W przypadku systemu macOS w wersji Mojave 10.14.x lub nowszej trzeba przyznać agentowi ochrony pełny dostęp do dysku, aby mógł wykonywać operacje tworzenia kopii zapasowych. Instrukcje można znaleźć w sekcji Przydzielanie uprawnienia „Dostęp do całego dysku" agentowi Cyber Protection (64657).
12. Aby korzystać z funkcji pulpitu zdalnego, przyznaj wymagane uprawnienia systemowe modułowi Agent rozwiązania Connect. Aby uzyskać więcej informacji, zobacz "Przyznawanie wymaganych uprawnień systemowych modułowi Agent rozwiązania Connect" (s. 83).

Odinstalowywanie agentów

Po odinstalowaniu agenta z obciążenia zostanie ono automatycznie usunięte z konsoli Cyber Protect. Jeśli obciążenie jest nadal widoczne po odinstalowaniu agenta, na przykład z powodu problemu z siecią, należy je ręcznie usunąć z konsoli. Dodatkowe informacje o tym, jak to zrobić, można znaleźć w sekcji "Usuwanie obciążeń z konsoli Cyber Protect" (s. 330).

Uwaga
Odinstalowanie agenta nie powoduje usunięcia żadnych planów ani kopii zapasowych.

Aby odinstalować agenta

Windows

1. Zaloguj się jako administrator na komputerze lub maszynie wirtualnej z agentem.
2. W **Panelu sterowania** przejdź do sekcji **Programy i funkcje** (**Dodaj lub usuń programy** w systemie Windows XP).
3. Kliknij **Acronis Cyber Protect** prawym przyciskiem myszy, a następnie wybierz **Odinstaluj**.
4. [W przypadku agenta chronionego hasłem] Podaj hasło wymagane do odinstalowania agenta, a następnie kliknij **Dalej**.
5. [Opcjonalnie] Zaznacz pole wyboru **Usuń dzienniki i ustawienia konfiguracji**.
   Jeśli planujesz zainstalować agenta ponownie, pozostaw to pole niezaznaczone. Jeśli zaznaczysz to pole wyboru, a następnie ponownie zainstalujesz agenta, obciążenie może zostać zduplikowane w konsoli Cyber Protect, a wówczas jego dawne kopie zapasowe nie zostaną z nim powiązane.
6. Kliknij **Odinstaluj**.

Linux

1. Na komputerze z agentem uruchom narzędzie `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` jako użytkownik root.
2. [Opcjonalnie] Zaznacz pole wyboru **Wyczyść wszystkie ślady produktu (usuń jego dzienniki, zadania, skarbce i ustawienia konfiguracji)**.
   Jeśli planujesz zainstalować agenta ponownie, pozostaw to pole niezaznaczone. Jeśli zaznaczysz to pole wyboru, a następnie ponownie zainstalujesz agenta, obciążenie może zostać zduplikowane w konsoli Cyber Protect, a wówczas jego dawne kopie zapasowe nie zostaną z nim

© Acronis International GmbH, 2003-2024

powiązane.

3. Potwierdź decyzję.

macOS

1. Na komputerze z agentem kliknij dwukrotnie plik instalacyjny .dmg.
2. Poczekaj, aż system operacyjny zamontuje instalacyjny obraz dysku.
3. W obrazie kliknij dwukrotnie **Odinstaluj**.
4. Jeśli pojawi się monit, podaj poświadczenia administratora.
5. Potwierdź decyzję.

Aby odinstalować komponenty dostępne w pakiecie z agentem dla systemu Windows

Można odinstalować wybrane komponenty dostępne w pakiecie z agentem dla systemu Windows, takie jak Cyber Protect Monitor, agent dla funkcji Zapobieganie utracie danych czy Bootable Media Builder, bez odinstalowywania agenta dla systemu Windows.

1. Zaloguj się jako administrator na komputerze lub maszynie wirtualnej z agentem.
2. Uruchom program instalacyjny, a następnie kliknij **Modyfikuj zainstalowane komponenty**.
3. Wyczyść pola wyboru obok komponentów, które chcesz odinstalować, a następnie kliknij **Gotowe**.

Aby usunąć agenta dla VMware (urządzenie wirtualne)

1. Korzystając z klienta vSphere, zaloguj się na serwerze vCenter.
2. [Jeśli urządzenie wirtualne jest włączone] Kliknij urządzenie wirtualne prawym przyciskiem myszy, a następnie kliknij **Zasilanie** > **Wyłącz**. Potwierdź decyzję.
3. [Jeśli urządzenie wirtualne korzysta z lokalnie podłączonej pamięci masowej w postaci dysku wirtualnego i chcesz zachować dane na tym dysku] Usuń wirtualną pamięć masową z urządzenia wirtualnego.
   a. Kliknij urządzenie wirtualne prawym przyciskiem myszy, a następnie kliknij **Edytuj ustawienia**.
   b. Wybierz dysk z magazynem i kliknij **Usuń**.
   c. W obszarze **Opcje usuwania** kliknij **Usuń z maszyny wirtualnej**.
   d. Kliknij **OK**.

   W wyniku tej operacji dysk pozostanie w magazynie danych. Dysk można podłączyć do innego urządzenia wirtualnego.
4. Kliknij urządzenie wirtualne prawym przyciskiem myszy, a następnie kliknij **Usuń z dysku**. Potwierdź decyzję.
5. [Opcjonalnie] [Jeśli nie planujesz ponownie korzystać z tego urządzenia] W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych** > **Lokalizacje**, a następnie usuń lokalizację odpowiadającą lokalnie podłączonej pamięci masowej.

© Acronis International GmbH, 2003-2024

Instalowanie i odinstalowywanie agentów ochrony przy użyciu interfejsu wiersza polecenia

Instalowanie i odinstalowywanie agentów ochrony w systemie Windows

W systemie Windows można przeprowadzić instalację nienadzorowaną lub dezinstalację na następujące sposoby:

- Za pomocą pliku EXE programu instalacyjnego i parametrów instalacji określonych w wierszu polecenia.
- Za pomocą pliku MSI wyodrębnionego z programu instalacyjnego i parametrów instalacji określonych w jeden z następujących sposobów:
  - W pliku MST
  - Bezpośrednio w wierszu polecenia

Instalacja nienadzorowana i odinstalowywanie przy użyciu pliku EXE

W przypadku tego typu instalacji nienadzorowanej należy pobrać program instalacyjny, a następnie uruchomić go z poziomu wiersza polecenia z wymaganymi parametrami instalacji. Z parametrami, których można użyć, można się zapoznać w sekcji "Parametry dotyczące instalacji nienadzorowanej (EXE)" (s. 94).

Nie trzeba wcześniej rozpakowywać pakietów instalacyjnych ani plików MSI i MST.

Instalowanie oraz odinstalowywanie agentów i komponentów (EXE)

Aby przeprowadzić instalację nienadzorowaną przy użyciu pliku EXE, uruchom program instalacyjny i podaj parametry instalacji w wierszu polecenia.

Aby pobrać program instalacyjny, w konsoli Cyber Protect kliknij ikonę konta widoczną w prawym górnym rogu, a następnie kliknij **Do pobrania**. Łącze pobierania jest też dostępne w panelu **Dodaj urządzenia**.

Aby zainstalować agenty i komponenty

1. Uruchom interfejs wiersza polecenia jako administrator, a następnie przejdź do pliku EXE programu instalacyjnego.
2. Aby uruchomić program instalacyjny i dodać parametry instalacji, uruchom następujące polecenie:

   ```
   <file path>/<EXE file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   Rozdziel parametry spacjami, a wartości parametrów — przecinkami bez spacji. Na przykład:

© Acronis International GmbH, 2003-2024

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,agentForSql,commandLine --install-dir="C:\Program
Files\BackupClient" --reg-address=https://eu2-cloud.company.com --reg-token=34F6-
8C39-4A5C --quiet
```

Dostępne parametry i ich wartości można znaleźć w sekcji "Parametry dotyczące instalacji nienadzorowanej (EXE)" (s. 94).

Przykłady

- Instalowanie agenta dla systemu Windows, agenta dla usługi Ochrona przed złośliwym oprogramowaniem, agenta dla usługi Filtrowanie adresów URL, narzędzia wiersza polecenia i narzędzia Cyber Protect Monitor. Rejestrowanie obciążenia w usłudze Cyber Protection przy użyciu nazwy użytkownika i hasła.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,agentForAmp,commandLine,trayMonitor --install-
  dir="C:\Program Files\BackupClient" --agent-account=system --reg-
  address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
  ```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia i narzędzia Cyber Protect Monitor. Tworzenie nowego konta logowania dla usługi agenta w systemie Windows. Rejestrowanie obciążenia w usłudze Cyber Protection przy użyciu tokenu.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,trayMonitor --install-dir="C:\Program
  Files\BackupClient" --agent-account=new --reg-address=https://eu2-cloud.company.com -
  -reg-token=34F6-8C39-4A5C
  ```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia, agenta dla bazy danych Oracle i narzędzia Cyber Protect Monitor. Rejestrowanie komputera w usłudze Cyber Protection przy użyciu nazwy użytkownika i hasła.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
  dir="C:\Program Files\BackupClient" --language=en --agent-account=system --reg-
  address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
  ```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia i narzędzia Cyber Protect Monitor. Ustawianie języka interfejsu użytkownika na niemiecki. Rejestrowanie komputera w usłudze Cyber Protection przy użyciu tokenu. Ustawienie serwera proxy HTTP.

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
  dir="C:\Program Files\BackupClient"--language=de --agent-account=system --reg-
  address=https://eu2-cloud.company.com --reg-token=34F6-8C39-4A5C --http-proxy-
  address=https://my-proxy.company.com:80 --http-proxy-login=tomsmith --http-proxy-
  password=tomspassword
  ```


© Acronis International GmbH, 2003-2024

Aby usunąć zainstalowany komponent

1. Uruchom interfejs wiersza polecenia jako administrator, a następnie przejdź do folderu `%ProgramFiles%\BackupClient\RemoteInstall`.
2. Uruchom następujące polecenie:

   ```
   web_installer.exe --remove-components=<value 1>,<value 2> --quiet
   ```

   Dostępne parametry i ich wartości można znaleźć w sekcji "Parametry dotyczące instalacji nienadzorowanej (EXE)" (s. 94).

Przykład

- Odinstalowywanie narzędzia Cyber Protect Monitor.

  ```
  C:\Program Files\BackupClient\RemoteInstall\web_installer.exe --remove-
  components=trayMonitor --quiet
  ```

Aby odinstalować agenta

1. Uruchom interfejs wiersza polecenia jako administrator, a następnie przejdź do folderu `%Program Files%\Common Files\Acronis\BackupAndRecovery`.
2. Uruchom następujące polecenie:

   ```
   Uninstaller.exe --quiet --delete-all-settings
   ```

   Dostępne parametry i ich wartości można znaleźć w sekcji "Parametry dotyczące instalacji nienadzorowanej (EXE)" (s. 94).

Przykłady

- Odinstalowywanie agenta dla systemu Windows i wszystkich jego komponentów. Usuwanie wszystkich dzienników, zadań i ustawień konfiguracyjnych.

  ```
  C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --quiet --
  delete-all-settings
  ```

- Odinstalowywanie chronionego hasłem agenta dla systemu Windows i wszystkich jego komponentów. Usuwanie wszystkich dzienników, zadań i ustawień konfiguracyjnych.

  ```
  C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-
  tamper-password=<password> --quiet --delete-all-settings
  ```

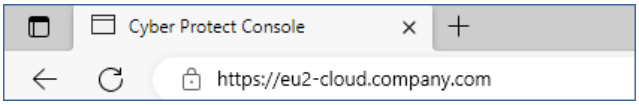
Parametry dotyczące instalacji nienadzorowanej (EXE)

W poniższej tabeli zestawiono parametry instalacji nienadzorowanej wykonywanej przy użyciu pliku EXE.

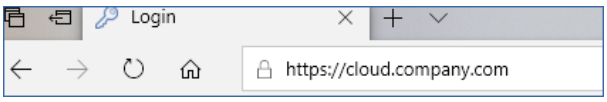
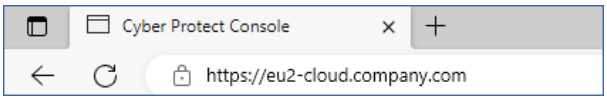
© Acronis International GmbH, 2003-2024

Parametry	Opis
Parametry ogólne	
`--add-components=` <komponent1,komponent2,...,komponentN>	Komponenty do zainstalowania. Pełną listę dostępnych komponentów można znaleźć w sekcji "Komponenty do instalacji nienadzorowanej (EXE)" (s. 99). W przypadku wpisywania kilku komponentów należy je rozdzielić przecinkami. Nie dodawaj spacji przed przecinkami ani po nich. W przypadku wpisania komponentów, które są już zainstalowane, zostaną one naprawione lub zaktualizowane, w zależności od wersji programu instalacyjnego i wersji zainstalowanych komponentów. Jeśli nie użyjesz tego parametru, zostanie zainstalowany domyślny zestaw komponentów, w zależności od komputera, na którym przeprowadzasz instalację. Na przykład agent dla SQL zostanie zainstalowany tylko na komputer z uruchomionym programem MS SQL Server.
`--install-dir=`<path>	Folder, w którym zostaną zainstalowane wybrane komponenty. Jeśli podany folder nie istnieje, zostanie utworzony. Jeśli ten parametr nie zostanie określony, zostanie użyty folder domyślny: `C:\Program Files\BackupClient`.
`--log-dir=`<path>	Folder, w którym będą zapisywane dzienniki instalacji. Jeśli ten parametr nie zostanie określony, zostanie użyty folder domyślny: `%ProgramData%\Acronis\InstallationLogs`.
`--language=`<kod>	Język programu. Dostępne są następujące wartości: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Jeśli ten parametr nie zostanie określony, a język systemu komputera, na którym jest przeprowadzana instalacja, znajduje się na powyższej liście, będzie używany język systemu. We wszystkich innych przypadkach zostanie ustawiona wartość en.
`--quiet`	Ten parametr umożliwia uruchomienie programu instalacyjnego bez wyświetlania graficznego interfejsu użytkownika. Nie należy go używać razem z parametrem `--register-`

© Acronis International GmbH, 2003-2024

Parametry	Opis
	`only`.
`--help`	Stosując ten parametr, możesz wyświetlić listę wszystkich dostępnych parametrów, których można użyć w wierszu polecenia — wraz z ich opisami.
`--fss-onboarding-auto-start`	Użyj tego parametru razem z parametrem `--quiet`, aby po instalacji nienadzorowanej został wyświetlony kreator wdrożenia usługi File Sync & Share.
Parametry rejestracji	
`--registration=`{skip | by-credentials | by-token | device-flow}	Ten parametr umożliwia wybranie sposobu rejestracji agenta po instalacji. Aby pominąć rejestrację, wpisz `skip`. Agenta możesz zarejestrować później przy użyciu parametru `--register-only`. Aby zarejestrować agenta przy użyciu poświadczeń, użyj parametru `by-credentials`, a następnie parametrów `--reg-login` i `--reg-password`. Możesz też użyć tylko parametrów `--reg-login` i `--reg-password`, a wówczas parametr `--registration=by-credentials` będzie opcjonalny. Aby zarejestrować agenta za pomocą tokenu rejestracji, należy podać parametr `by-token`, a następnie użyć parametru `--reg-token`. Możesz też użyć tylko parametru `--reg-token`, a wówczas parametr `--registration=by-token` będzie opcjonalny. Aby zarejestrować agenta przy użyciu protokołu OAuth 2.0, określ parametr `device-flow`. Po zakończeniu instalacji zostanie automatycznie otwarta strona rejestracji. W przypadku użycia parametru `--registration=device-flow` podaj dokładny adres centrum danych jako wartość parametru `--reg-address`. Jest to adres URL widoczny **po zalogowaniu się** do usługi Cyber Protection. Na przykład `https://ue2-chmura.nazwa_firmy.com.pl`.  Nie używaj parametru `--registration=device-flow` z parametrem `--quiet`.
`--reg-address=`<adres url>	Adres URL usługi Cyber Protection. Możesz użyć tego

© Acronis International GmbH, 2003-2024

Parametry	Opis
	parametru albo z parametrami `--reg-login` i `--reg-password`, albo z parametrem `--reg-token`. • W przypadku używania go z parametrami `--reg-login` i `--reg-password` podaj adres używany do **logowania się** w usłudze Cyber Protection. Na przykład `https://cloud.company.com`:  • W przypadku używania go z parametrem `--reg-token` podaj dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do usługi Cyber Protection. Na przykład `https://eu2-cloud.company.com`.  Nie używaj adresu `https://cloud.company.com` z parametrem `--reg-token`.
`--reg-login=`<login> `--reg-password=`<password>	Poświadczenia dostępu do konta, na którym zostanie zarejestrowany agent w usłudze Cyber Protection. Nie może to być konto administratora partnera. W przypadku użycia tych parametrów określenie parametru `--registration` jest opcjonalne. Nie używaj tych parametrów razem z parametrem `--reg-token`.
`--reg-token=`<token>	Token rejestracji. Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Dokładniejsze instrukcje dotyczące generowania tokenu można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129). W przypadku użycia tego parametru określenie parametru `--registration` jest opcjonalne. Nie używaj tego parametru z parametrami `--reg-login` i `--reg-password`.
`--register-only`	Użyj tego parametru, aby pominąć instalację i zarejestrować agenta przy użyciu protokołu OAuth 2.0 (device-flow). Po zakończeniu instalacji zostanie automatycznie otwarta strona rejestracji.

© Acronis International GmbH, 2003-2024

Parametry	Opis
	Nie używaj parametru `--register-only` z parametrem `--quiet`.
Konto logowania dla usługi agenta	
`--agent-account`={system | new | custom} lub `--agent-account-login`=<login> `--agent-account-password`=<password>	Ten parametr umożliwia wskazanie konta logowania, na którym będzie działać usługa agenta. Dodatkowe informacje o kontach logowania można znaleźć w sekcji "Zmienianie konta logowania na komputerach z systemem Windows" (s. 86). Aby skorzystać z konta **System lokalny**, określ parametr `--agent-account=system` lub nie używaj parametru `--agent-account` w poleceniu. Aby usługa agenta działała na nowym koncie logowania o nazwie **Acronis Agent User**, które jest tworzone automatycznie, określ parametr `new`. Aby usługa agenta działała w ramach istniejącego już konta, dodaj poświadczenia dostępu do konta za pomocą parametrów `--agent-account-login` (w przypadku nazwy logowania) i `--agent-account-password` (w przypadku hasła). W takiej sytuacji określenie parametru `--agent-account=custom` jest opcjonalne.
Parametry dotyczące vCenter/ESXi	
`--esxi-address`=<host>	Nazwa hosta lub adres IP serwera vCenter lub hosta ESXi. Tego parametru należy użyć w przypadku instalacji agenta dla VMware.
`--esxi-login`=<login> `--esxi-password`=<password>	Poświadczenia dostępu do serwera vCenter lub hosta ESXi. Tych parametrów należy użyć w przypadku instalacji agenta dla VMware.
Parametry dotyczące serwera proxy	
`--http-proxy`={none | system | custom}	Ten parametr służy do określenia serwera proxy HTTP, który ma być używany do tworzenia kopii zapasowych w chmurze i odzyskiwania z chmury. Jeśli połączenia z serwerem proxy mają być wyłączone, określ `--http-proxy=none`. Aby użyć ogólnosystemowego serwera proxy, określ parametr `--http-proxy=system` lub nie używaj parametru

© Acronis International GmbH, 2003-2024

Parametry	Opis
	`--http-proxy` w poleceniu. Aby użyć innego serwera proxy, określ adres serwera proxy i poświadczenia dostępu do niego przy użyciu parametrów `--http-proxy-address`, `--http-proxy-login` i `--http-proxy-password`. W takiej sytuacji określenie parametru `--http-proxy=custom` jest opcjonalne.
`--http-proxy-address=`<host>:<port>	Nazwa hosta lub adres IP oraz port niestandardowego serwera proxy HTTP.
`--http-proxy-login=`<login>	Nazwa logowania niestandardowego serwera proxy HTTP.
`--http-proxy-password=`<password>	Hasło niestandardowego serwera proxy HTTP.
Parametry dezinstalacji	
`--remove-components=`<komponent1,komponent2,...,komponentN>	Komponenty do odinstalowania. Pełną listę dostępnych komponentów można znaleźć w sekcji "Komponenty do instalacji nienadzorowanej (EXE)" (s. 99). W przypadku wpisywania kilku komponentów należy je rozdzielić przecinkami. Nie dodawaj spacji przed przecinkami ani po nich. **Ważne** Za pomocą tego parametru można odinstalować tylko komponenty. Aby całkowicie odinstalować produkt, wybierz Panel sterowania systemu Windows > Programy i funkcje, wybierz produkt, a następnie kliknij **Odinstaluj**.
`--delete-all-settings`	Użyj tego opcjonalnego parametru, gdy używasz parametru `--remove-components` w celu usunięcia wszystkich dzienników produktu, zadań i ustawień konfiguracji.
`--anti-tamper-password=`<password>	Hasło wymagane do odinstalowania chronionego hasłem agenta dla systemu Windows lub modyfikacji jego składników.

Komponenty do instalacji nienadzorowanej (EXE)

Poniższa tabela zawiera zestawienie komponentów, których można użyć do instalacji nienadzorowanej wykonywanej przy użyciu pliku EXE. Użyj tych nazw jako wartości parametru `--add-components`.

© Acronis International GmbH, 2003-2024

Dodatkowe informacje można znaleźć w sekcji "Parametry dotyczące instalacji nienadzorowanej (EXE)" (s. 94)"Parametry dotyczące instalacji nienadzorowanej (MSI)" (s. 104)

Nazwa wartości	Opis komponentu
`agentForWindows`	Agent dla systemu Windows
`agentForSas`	Agent dla usługi File Sync & Share
`agentForAd`	Agent dla usługi Active Directory
`agentForAmp`	Agent dla usługi Ochrona przed złośliwym oprogramowaniem i agent dla usługi Filtrowanie adresów URL
`agentForDlp`	Agent dla rozwiązania Data Loss Prevention
`agentForEsx`	Agent dla VMware (Windows)
`agentForExchange`	Agent dla programu Exchange
`agentForHyperV`	Agent dla Hyper-V
`agentForOffice365`	Agent dla usługi Office 365
`agentForOracle`	Agent dla programu Oracle
`agentForSql`	Agent dla SQL
`commandLine`	Narzędzie wiersza polecenia
`mediaBuilder`	Generator nośnika startowego
`trayMonitor`	Cyber Protect Monitor
`all`	Ta wartość obejmuje wszystkie komponenty.
`allAgents`	Ta wartość obejmuje wszystkie agenty.

Instalacja nienadzorowana i odinstalowywanie przy użyciu pliku MSI

Na potrzeby instalacji nienadzorowanej tego typu należy użyć Instalatora Windows (programu `Msiexec`). Wyodrębnij wcześniej pakiety instalacyjne oraz plik MSI, korzystając z graficznego interfejsu użytkownika programu instalacyjnego.

W przypadku instalowania komponentów za pomocą pliku MSI możesz użyć pliku transformacji MST w celu dostosowania parametrów instalacji. Dodatkowe informacje na temat korzystania z zarówno pliku MSI, jaki i pliku MST można znaleźć w sekcji "Instalowanie agentów i komponentów (połączenie MSI i MST)" (s. 101). Tej metody instalacji można użyć w domenie Active Directory w celu zainstalowania agentów ochrony przy użyciu zasad grupy systemu Windows. Aby uzyskać więcej informacji, zobacz "Wdrażanie agentów ochrony przy użyciu zasad grupy" (s. 143).

© Acronis International GmbH, 2003-2024

Parametry instalacji można też dodać ręcznie w wierszu polecenia. W tym przypadku nie trzeba korzystać z pliku MST. Aby uzyskać więcej informacji, zobacz "Przykłady" (s. 102).

Wyodrębnianie plików MSI, MST i CAB

Wyodrębnij pliki MSI, MST i CAB z pakietami instalacyjnymi przez uruchomienie graficznego interfejsu użytkownika programu instalacyjnego.

Aby wyodrębnić pliki MSI, MST i CAB

1. Uruchom graficzny interfejs użytkownika programu instalacyjnego, a następnie kliknij **Utwórz pliki .mst i .msi na potrzeby instalacji nienadzorowanej**.
2. W polu **Elementy do zainstalowania** wybierz komponenty, które chcesz zainstalować, a następnie kliknij **Gotowe**.

   Z programu instalacyjnego zostaną wyodrębnione pakiety instalacyjne tych komponentów jako pliki CAB.
3. W polu **Ustawienia rejestracji** wybierz **Użyj poświadczeń** lub **Użyj tokenu rejestracji**. W zależności od wyboru określ poświadczenia lub token rejestracji, a następnie kliknij **Gotowe**.

   Dodatkowe instrukcje dotyczące generowania tokenu rejestracji można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129).
4. [Tylko w przypadku instalowania na kontrolerze domeny] W obszarze **Konto logowania dla usługi agenta** wybierz **Użyj następującego konta**. Określ konto użytkownika, które będzie służyć do uruchamiania usługi agenta, a następnie kliknij **Gotowe**. Ze względów bezpieczeństwa program instalacyjny nie tworzy automatycznie nowych kont na kontrolerze domeny.

   Uwaga
   Wskazane konto użytkownika musi mieć przyznane prawo `Logowanie jako usługa`. Konto to musi już być używane na kontrolerze domeny, aby jego folder profilu został utworzony na tym komputerze.

   Dodatkowe informacje o instalowaniu agenta na kontrolerze domeny w trybie tylko do odczytu można znaleźć w tym artykule z bazy wiedzy Knowledge Base.
5. Przejrzyj lub zmodyfikuj inne ustawienia instalacji, które zostaną dodane do pliku MST, a następnie kliknij **Kontynuuj**.
6. Wybierz folder, do którego zostaną wyodrębnione pliki MSI, MST i CAB, a następnie kliknij **Wygeneruj**.

Instalowanie agentów i komponentów (połączenie MSI i MST)

Użyj pliku MST w celu dostosowania ustawień instalacji dla pliku MSI. Użyj zarówno pliku MSI, jak i MST w przypadku instalowania agentów na wielu komputerach przy użyciu zasad grupy systemu Windows. Aby uzyskać więcej informacji, zobacz "Wdrażanie agentów ochrony przy użyciu zasad grupy" (s. 143).

Aby zainstalować komponenty przy użyciu plików MSI i MST

© Acronis International GmbH, 2003-2024

1. Wyodrębnij pliki MSI i MST zgodnie z opisem podanym w sekcji "Wyodrębnianie plików MSI, MST i CAB" (s. 101).
2. W interfejsie wiersza polecenia komputera, na którym chcesz zainstalować komponenty, uruchom następujące polecenie:

   ```
   msiexec /i <MSI file> TRANSFORMS=<MST file>
   ```

   Na przykład:

   ```
   msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
   ```

Instalowanie oraz odinstalowywanie agentów i komponentów (MSI i wybór bezpośredni)

Uruchom plik MSI, ręcznie wybierz komponenty do zainstalowania i dodaj parametry ich instalacji w wierszu polecenia. W tym przypadku nie trzeba korzystać z pliku MST.

Aby zainstalować agenty i komponenty

1. Wyodrębnij plik MSI i pakiety instalacyjne (pliki CAB) zgodnie z opisem podanym w sekcji "Wyodrębnianie plików MSI, MST i CAB" (s. 101).
   Do instalacji tą metodą są potrzebne tylko pliki MSI i CAB. Nie trzeba korzystać z pliku MST.
2. W interfejsie wiersza polecenia komputera uruchom następujące polecenie:

   ```
   msiexec /i <MSI file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   Rozdziel parametry spacjami, a wartości parametrów — przecinkami bez spacji. Na przykład:

   ```
   msiexec.exe /i BackupClient64.msi
   ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
   TARGETDIR="C:\Program Files\BackupClient" REGISTRATION_ADDRESS=https://eu2-
   cloud.company.com REGISTRATION_TOKEN=34F6-8C39-4A5C
   ```

   Dostępne parametry i ich wartości można znaleźć w sekcji "Parametry dotyczące instalacji nienadzorowanej (MSI)" (s. 104).

Przykłady

- Instalowanie agenta dla systemu Windows, agenta dla usługi Ochrona przed złośliwym oprogramowaniem, agenta dla usługi Filtrowanie adresów URL, narzędzia wiersza polecenia i narzędzia Cyber Protect Monitor. Rejestrowanie obciążenia w usłudze Cyber Protection przy użyciu nazwy użytkownika i hasła.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,CommandLineTool,Tray
  Monitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_
  SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_
  LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
  ```


© Acronis International GmbH, 2003-2024

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia i narzędzia Cyber Protect Monitor. Tworzenie nowego konta logowania dla usługi agenta w systemie Windows. Rejestrowanie obciążenia w usłudze Cyber Protection przy użyciu tokenu.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
  ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
  8C39-4A5C
  ```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia, agenta dla bazy danych Oracle i narzędzia Cyber Protect Monitor. Rejestrowanie komputera w usłudze Cyber Protection przy użyciu nazwy użytkownika i hasła zakodowanego w formacie base64. Jeśli hasło zawiera znaki specjalne lub spacje, może być konieczne jego zakodowanie. Dokładniejsze instrukcje dotyczące kodowania hasła można znaleźć w sekcji "Używanie haseł ze znakami specjalnymi lub spacjami" (s. 133).

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
  rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
  LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
  REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
  ```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia i narzędzia Cyber Protect Monitor. Rejestrowanie komputera w usłudze Cyber Protection przy użyciu tokenu. Ustawienie serwera proxy HTTP.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
  MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
  REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
  HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
  ```

Aby usunąć zainstalowany komponent

1. Wyodrębnij plik MSI i pakiety instalacyjne (pliki CAB) zgodnie z opisem podanym w sekcji "Wyodrębnianie plików MSI, MST i CAB" (s. 101).

   Do instalacji tą metodą są potrzebne tylko pliki MSI i CAB. Nie trzeba korzystać z pliku MST.
2. W interfejsie wiersza polecenia komputera uruchom następujące polecenie:

   ```
   msiexec /i <MSI file><REMOVE>=<value 1>,<value 2> REBOOT=ReallySuppress /qn
   ```

   Dostępne parametry i ich wartości można znaleźć w sekcji "Parametry dotyczące instalacji nienadzorowanej (MSI)" (s. 104).

© Acronis International GmbH, 2003-2024

Przykład

- Usuwanie monitora Cyber Protect.

```
msiexec.exe /i BackupClient64.msi /l*v uninstall_log.txt REMOVE=TrayMonitor
REBOOT=ReallySuppress /qn
```

Aby odinstalować agenta

1. Wyodrębnij plik MSI i pakiety instalacyjne (pliki CAB) zgodnie z opisem podanym w sekcji "Wyodrębnianie plików MSI, MST i CAB" (s. 101).

   Do instalacji tą metodą są potrzebne tylko pliki MSI i CAB. Nie trzeba korzystać z pliku MST.
2. W interfejsie wiersza polecenia komputera uruchom następujące polecenie:

   ```
   msiexec /x <MSI file> /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
   REBOOT=ReallySuppress /qn
   ```

   Dostępne parametry i ich wartości można znaleźć w sekcji "Parametry dotyczące instalacji nienadzorowanej (MSI)" (s. 104).

Przykłady

- Odinstalowywanie agenta dla systemu Windows i wszystkich jego komponentów. Usuwanie wszystkich dzienników, zadań i ustawień konfiguracyjnych.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
REBOOT=ReallySuppress /qn
```

- Odinstalowywanie chronionego hasłem agenta dla systemu Windows i wszystkich jego komponentów. Usuwanie wszystkich dzienników, zadań i ustawień konfiguracyjnych.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt ANTI_TAMPER_
PASSWORD=<password> DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress /qn
```

Parametry dotyczące instalacji nienadzorowanej (MSI)

W poniższej tabeli zestawiono parametry instalacji nienadzorowanej wykonywanej przy użyciu pliku MSI.

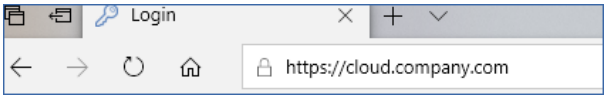
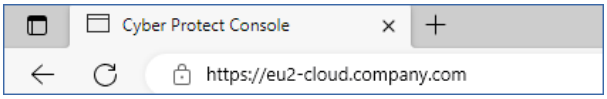
Możesz też użyć dodatkowych parametrów polecenia `msiexec`. Na przykład parametr `/qn` pozwala zapobiegać wyświetlaniu jakichkolwiek elementów graficznego interfejsu użytkownika. Dodatkowe informacje na temat parametrów polecenia `msiexec` można znaleźć w dokumentacji firmy Microsoft.

Parametry	Opis
Parametry ogólne	
`ADDLOCAL=`	Komponenty do zainstalowania. Pełną listę dostępnych

© Acronis International GmbH, 2003-2024

Parametry	Opis
<komponent1,komponent2,...,komponentN>	komponentów można znaleźć w sekcji "Komponenty do instalacji nienadzorowanej (MSI)" (s. 108). W przypadku wpisywania kilku komponentów należy je rozdzielić przecinkami. Nie dodawaj spacji przed przecinkami ani po nich. **Uwaga** Musisz wyodrębnić pliki instalacyjne wszystkich komponentów, które chcesz zainstalować. Dokładniejsze instrukcje dotyczące ich wyodrębniania można znaleźć w sekcji "Wyodrębnianie plików MSI, MST i CAB" (s. 101).
`TARGETDIR=`<path>	Folder, w którym zostaną zainstalowane wybrane komponenty. Jeśli podany folder nie istnieje, zostanie utworzony. Jeśli ten parametr nie zostanie określony, zostanie użyty folder domyślny: `C:\Program Files\BackupClient`.
`REBOOT=ReallySuppress`	Dodaj ten parametr, jeśli chcesz zainstalować komponenty bez ponownego uruchamiania urządzenia.
`/l*v` <log file>	Podaj ten parametr, aby zapisać pełny dziennik. Dziennik ten jest potrzebny, jeśli zajdzie potrzeba zbadania problemów z instalacją.
`CURRENT_LANGUAGE=`<language ID>	Język programu. Dostępne są następujące wartości: en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW. Jeśli ten parametr nie zostanie określony, a język systemu komputera, na którym jest przeprowadzana instalacja, znajduje się na powyższej liście, będzie używany język systemu. We wszystkich innych przypadkach zostanie ustawiona wartość en.
`SKIP_SHA2_KB_CHECK={0,1}`	Użyj tego parametru, aby narzędzie sprawdziło, czy na komputerze jest zainstalowana aktualizacja obsługi podpisywania kodu przy użyciu algorytmu SHA2 od firmy Microsoft (KB4474419). Ta operacja sprawdzania działa tylko w systemach operacyjnych, które wymagają tej aktualizacji. W celu sprawdzenia, czy jest ona wymagana w przypadku danego systemu operacyjnego, zobacz "Obsługiwane systemy operacyjne i środowiska" (s. 23).

© Acronis International GmbH, 2003-2024

Parametry	Opis
	Użyj tego parametru z wartością `1`, aby pominąć to sprawdzanie. Jeśli nie określisz tego parametru lub ustawisz jego wartość na `0`, a aktualizacja obsługi podpisywania kodu przy użyciu algorytmu SHA2 nie zostanie znaleziona na komputerze, instalacja się nie powiedzie.
`FSS_ONBOARDING_AUTO_START={0,1}`	Użyj tego parametru z wartością `1`, aby po instalacji nienadzorowanej został wyświetlony kreator wdrożenia usługi File Sync & Share. Jeśli nie dodasz tego parametru lub ustawisz jego wartość na `0`, kreator wdrożenia nie zostanie wyświetlony.
Parametry rejestracji	
`REGISTRATION_ADDRESS`	Adres URL usługi Cyber Protection. Tego parametru można użyć albo z parametrami `REGISTRATION_LOGIN` i `REGISTRATION_PASSWORD`, albo z parametrem `REGISTRATION_TOKEN`. • W przypadku użycia parametru z parametrami `REGISTRATION_LOGIN` i `REGISTRATION_PASSWORD` należy podać adres używany **do logowania się** w usłudze Cyber Protection. Na przykład `https://cloud.company.com`:  • W przypadku użycia tego parametru z parametrem `REGISTRATION_TOKEN` podaj dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do usługi Cyber Protection. Na przykład `https://eu2-cloud.company.com`.  Nie używaj adresu `https://cloud.company.com` z parametrem `REGISTRATION_TOKEN`.

`REGISTRATION_LOGIN`
 	
`REGISTRATION_PASSWORD`
	Poświadczenia dostępu do konta, na którym zostanie zarejestrowany agent w usłudze Cyber Protection. Nie może to być konto administratora partnera.
	
	Nie używaj tych parametrów razem z parametrem `REGISTRATION_TOKEN`.

© Acronis International GmbH, 2003-2024

Parametry	Opis
REGISTRATION_PASSWORD_ENCODED	Hasło do konta, na którym zostanie zarejestrowany agent w usłudze Cyber Protection, zakodowane w formacie base64. Dodatkowe informacje o procedurze kodowania hasła można znaleźć w sekcji "Używanie haseł ze znakami specjalnymi lub spacjami" (s. 133).
REGISTRATION_TOKEN	Token rejestracji. Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Dokładniejsze instrukcje dotyczące generowania tokenu można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129). Nie używaj tego parametru z parametrami REGISTRATION_LOGIN i REGISTRATION_PASSWORD.
REGISTRATION_REQUIRED={0,1}	Użyj tego parametru, aby określić, co się stanie w razie niepowodzenia rejestracji. W przypadku ustawienia wartości 1 instalacja również się nie powiedzie. W przypadku ustawienia wartości 0 lub nieokreślenia parametru instalacja zakończy się pomyślnie, nawet jeśli rejestracja się nie powiedzie.
Konto logowania dla usługi agenta	
MMS_USE_SYSTEM_ACCOUNT={0,1}	Użyj tego parametru z wartością 1, aby usługa działała na koncie logowania **System lokalny**. Dodatkowe informacje o kontach logowania można znaleźć w sekcji "Zmienianie konta logowania na komputerach z systemem Windows" (s. 86).
MMS_CREATE_NEW_ACCOUNT={0,1}	Użyj tego parametru z wartością 1, aby usługa agenta działała na nowym koncie logowania o nazwie **Acronis Agent User**, które jest tworzone automatycznie.
MMS_SERVICE_USERNAME=<user name> MMS_SERVICE_PASSWORD=<password>	Użyj tych parametrów, aby wskazać już istniejące konto logowania, na którym będzie działać usługa agenta.
Parametry dotyczące vCenter/ESXi	
SET_ESX_SERVER={0,1}	Tego parametru należy użyć w przypadku instalacji agenta dla VMware. W przypadku ustawienia wartości 0 nie będzie ustanawiane połączenie między agentem dla VMware a serwerem vCenter lub hostem ESXi. W przypadku ustawienia wartości 1 dodaj następujące

© Acronis International GmbH, 2003-2024

Parametry	Opis
	parametry: ESX_HOST, EXI_USER, ESX_PASSWORD.
ESX_HOST=<host name>	Nazwa hosta lub adres IP serwera vCenter lub hosta ESXi.
ESX_USER=<user name> ESX_PASSWORD=<password>	Poświadczenia dostępu do serwera vCenter lub hosta ESXi.
Parametry dotyczące serwera proxy	
HTTP_PROXY_ADDRESS=<IP address> HTTP_PROXY_PORT=<port>	Użyj tych parametrów, aby wskazać serwer proxy HTTP, którego będzie używać agent. Jeśli nie korzystasz z serwera proxy, nie podawaj tych parametrów.
HTTP_PROXY_LOGIN=<login> HTTP_PROXY_PASSWORD=<password>	Poświadczenia dostępu do serwera proxy HTTP. Jeśli serwer proxy wymaga uwierzytelniania, należy użyć tych parametrów.
Parametry dezinstalacji	
REMOVE={<list of components>|ALL}	Komponenty do odinstalowania. W przypadku wpisywania kilku komponentów należy je rozdzielić przecinkami. Nie dodawaj spacji przed przecinkami ani po nich. Aby usunąć wszystkie komponenty produktu, ustaw wartość ALL.
DELETE_ALL_SETTINGS={0, 1}	Aby usunąć wszystkie dzienniki produktu, zadania i ustawienia konfiguracji, ustaw wartość 1. Użyj tego opcjonalnego parametru, jeśli używasz parametru REMOVE.
ANTI_TAMPER_PASSWORD=<password>	Hasło wymagane do odinstalowania chronionego hasłem agenta dla systemu Windows lub modyfikacji jego składników.

Komponenty do instalacji nienadzorowanej (MSI)

Poniższa tabela zawiera zestawienie komponentów, których można użyć do instalacji nienadzorowanej wykonywanej przy użyciu pliku MSI. Użyj tych nazw jako wartości parametru ADDLOCAL. Aby uzyskać więcej informacji, zobacz "Parametry dotyczące instalacji nienadzorowanej (MSI)" (s. 104).

Nazwa wartości	Opis	Inne wymagane	Bitowość

© Acronis International GmbH, 2003-2024

	komponentu	równolegle komponenty	
AgentFeature	Podstawowe komponenty dla agentów		wersja 32-bitowa/64-bitowa
MmsMspComponents	Podstawowe komponenty na potrzeby tworzenia kopii zapasowych	AgentFeature	wersja 32-bitowa/64-bitowa
BackupAndRecoveryAgent	Agent dla systemu Windows	MmsMspComponents	wersja 32-bitowa/64-bitowa
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa
DlpAgentFeature	Agent dla rozwiązania Data Loss Prevention	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa
SasAgentFeature	Agent dla usługi File Sync & Share	TrayMonitor	wersja 32-bitowa/64-bitowa
ArxAgentFeature	Agent dla programu Exchange	MmsMspComponents	wersja 32-bitowa/64-bitowa
ArsAgentFeature	Agent dla SQL	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa
ARADAgentFeature	Agent dla usługi Active Directory	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa
ArxOnlineAgentFeature	Agent dla usługi Microsoft 365	MmsMspComponents	wersja 32-bitowa/64-bitowa
OracleAgentFeature	Agent dla programu	BackupAndRecoveryAgent	wersja 32-bitowa/64-

© Acronis International GmbH, 2003-2024

	Oracle		bitowa
AcronisESXSupport	Agent dla VMware ESX(i) (Windows)	BackupAndRecoveryAgent	64-bitowy
HyperVAgent	Agent dla Hyper-V	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa
CommandLineTool	Narzędzie wiersza polecenia		wersja 32-bitowa/64-bitowa
TrayMonitor	Cyber Protect Monitor	AgentFeature	wersja 32-bitowa/64-bitowa
BackupAndRecoveryBootableComponents	Generator nośnika startowego		wersja 32-bitowa/64-bitowa

Instalowanie i odinstalowywanie agentów ochrony w systemie Linux

W tej sekcji opisano, jak zainstalować lub odinstalować agenty ochrony w trybie nienadzorowanym na komputerze z systemem Linux przy użyciu wiersza polecenia.

Aby zainstalować agenta

1. Otwórz terminal.

2. Wykonaj jedną z następujących czynności:

- Aby rozpocząć instalację przez podanie parametrów w wierszu polecenia, uruchom następujące polecenie:

  ```
  <package name> -a <parameter 1> ... <parameter N>
  ```

  Zmienna <package name> oznacza nazwę pakietu instalacyjnego (pliku .i686 lub .x86_64) Wszystkie dostępne parametry i ich wartości opisano w sekcji "Parametry instalacji nienadzorowanej lub dezinstalacji" (s. 112).
- Aby rozpocząć instalację z parametrami podanymi w osobnym pliku tekstowym, uruchom następujące polecenie:

  ```
  <package name> -a --options-file=<path to the file>
  ```

  Ten sposób może się przydać, jeśli nie chcesz wprowadzać informacji wrażliwych w wierszu polecenia. W takiej sytuacji możesz określić ustawienia konfiguracyjne w osobnym pliku tekstowym i dopilnować, aby nikt inny nie miał do nich dostępu. Umieść każdy parametr w osobnym wierszu wraz z wartością danego parametru, na przykład:

 © Acronis International GmbH, 2003-2024

```
--rain=https://cloud.company.com
--login=johndoe
--password=johnspassword
--auto
```

lub

```
-C
https://cloud.company.com
-g
johndoe
-w
johnspassword
-a
--language
en
```

Jeśli jakiś parametr zostanie określony zarówno w wierszu polecenia, jak i w pliku tekstowym, zostanie użyta wartość z wiersza polecenia.

3. Jeśli na komputerze jest włączona funkcja UEFI Secure Boot, pojawi się informacja o konieczności ponownego uruchomienia systemu po zakończeniu instalacji. Koniecznie zapamiętaj, jakiego hasła (hasła użytkownika root czy „acronis") należy użyć. Podczas ponownego uruchamiania systemu wybierz opcję zarządzania kluczem właściciela komputera, zaznacz **Zarejestruj klucz właściciela komputera**, a następnie zarejestruj klucz przy użyciu zalecanego hasła.

Jeśli po instalacji agenta zostanie włączona funkcja UEFI Secure Boot, powtórz instalację, w tym krok 3. W przeciwnym razie następne operacje tworzenia kopii zapasowej zakończą się niepowodzeniem.

Aby odinstalować agenta

1. Otwórz terminal.
2. Wykonaj jedną z następujących czynności:
   - Aby odinstalować agenta i usunąć wszystkie dzienniki, zadania oraz ustawienia konfiguracyjne, uruchom następujące polecenie:

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a
     ```

   - Aby odinstalować agenta, ale zachować jego identyfikator (jeśli na przykład zamierzasz później zainstalować tego agenta), uruchom następujące polecenie:

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a --no-purge
     ```

   - Aby odinstalować agenta przy użyciu pliku instalacyjnego, uruchom następujące polecenie:

     ```
     <package name> -a -u
     ```


© Acronis International GmbH, 2003-2024

Zmienna <package name> oznacza nazwę pakietu instalacyjnego (pliku .i686 lub .x86_64) Wszystkie dostępne parametry i ich wartości opisano w sekcji "Parametry instalacji nienadzorowanej lub dezinstalacji" (s. 112).

Uwaga
Tego polecenia należy używać tylko wtedy, gdy pakiet instalacyjny jest w tej samej wersji co zainstalowany agent i jeśli plik `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` jest uszkodzony lub niedostępny.

Parametry instalacji nienadzorowanej lub dezinstalacji

W tej sekcji opisano parametry używane podczas instalacji nienadzorowanej lub dezinstalacji w systemie Linux.

Minimalna konfiguracja na potrzeby instalacji nienadzorowanej obejmuje parametr `-a` i parametry rejestracji (na przykład `--login` i `--password`; `--rain` i `--token`). Możesz użyć więcej parametrów, aby dostosować instalację do swoich potrzeb.

Parametry instalacji

Podstawowe parametry

`{-i |--id=}<list of components>`

Nazwy komponentów do zainstalowania, rozdzielone przecinkami bez spacji. W pakiecie instalacyjnym .x86_64 dostępne są następujące komponenty do zainstalowania:

Komponent	Opis komponentu
BackupAndRecoveryAgent	Agent dla systemu Linux
AgentForPCS	Agent dla Virtuozzo
OracleAgentFeature	Agent dla programu Oracle
MySQLAgentFeature	Agent dla MySQL/MariaDB

W przypadku nieokreślenia tego parametru zostaną zainstalowane wszystkie powyższe komponenty.

Agent dla Virtuozzo, agent dla programu Oracle i agent dla MySQL/MariaDB wymagają zainstalowania również agenta dla systemu Linux.

Pakiet instalacyjny .i686 zawiera tylko agenta BackupAndRecoveryAgent.

`{-a|--auto}`

Proces instalacji i rejestracji zostanie zakończony bez dodatkowych działań użytkownika. Korzystając z tego parametru, należy wskazać konto, na którym agent zostanie zarejestrowany w usłudze Cyber Protection — albo przy użyciu parametru `--token`, albo przy użyciu parametrów `--login` i `--password`.

© Acronis International GmbH, 2003-2024

`{-t|--strict}`

W przypadku określenia tego parametru wystąpienie ostrzeżenia podczas instalacji poskutkuje niepowodzeniem instalacji. W przypadku nieokreślenia tego parametru instalacja zostanie pomyślnie ukończona nawet w razie wystąpienia ostrzeżeń.

`{-n|--nodeps}`

Brak wymaganych pakietów systemu Linux zostanie zignorowany podczas instalacji.

`{-d|--debug}`

Dziennik instalacji zostanie zapisany w trybie informacji pełnej.

`--options-file=<location>`

Parametry instalacji zostaną odczytane z pliku tekstowego zamiast z wiersza polecenia.

`--language=<language ID>`

Język programu. Dostępne są następujące wartości: `en`, `bg`, `cs`, `da`, `de`, `es`, `fr`, `hu`, `id`, `it`, `ja`, `ko`, `ms`, `nb`, `nl`, `pl`, `pt`, `pt_BR`, `ru`, `fi`, `sr`, `sv`, `tr`, `zh`, `zh_TW`.
Jeśli ten parametr nie zostanie określony, język produktu zostanie zdefiniowany na podstawie języka systemu, pod warunkiem, że znajduje się on na powyższej liście. Jeśli go nie ma, język produktu zostanie ustawiony na język angielski (`en`).

Parametry rejestracji

Określ jeden z następujących parametrów:

- `{-g|--login=}<user name>` i `{-w|--password=}<password>`

  Poświadczenia dostępu do konta, na którym zostanie zarejestrowany agent w usłudze Cyber Protection. Nie może to być konto administratora partnera.

- `--token=<token>`

  Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Można go wygenerować w konsoli Cyber Protect zgodnie z instrukcją podaną w sekcji "Wdrażanie agentów ochrony przy użyciu zasad grupy" (s. 143).

  Parametru `--token` nie można używać razem z parametrami `--login`, `--password` i `--register-with-credentials`.

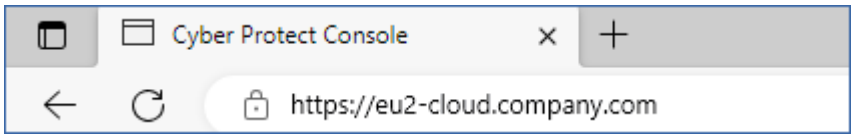
  - `{-C|--rain=}<service address>`

    Adres URL usługi Cyber Protection.

    Jeśli do rejestracji zostaną użyte parametry `--login` i `--password`, to nie trzeba jawnie podawać powyższego parametru, ponieważ instalator domyślnie użyje właściwego adresu — tego, którego używasz **do logowania się** do usługi Cyber Protection. Na przykład:

© Acronis International GmbH, 2003-2024

Jednak w przypadku użycia parametru `{-C|--rain=}` z parametrem `--token` trzeba podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do usługi Cyber Protection. Na przykład:



- `--register-with-credentials`

W przypadku podania tego parametru zostanie uruchomiony graficzny interfejs instalatora. Aby ukończyć rejestrację, należy wprowadzić nazwę użytkownika i hasło do konta, na którym agent zostanie zarejestrowany w usłudze Cyber Protection. Nie może to być konto administratora partnera.

- `--skip-registration`

Użyj tego parametru, jeśli chcesz zainstalować agenta, ale planujesz go zarejestrować w usłudze Cyber Protection później. Aby uzyskać więcej informacji, jak to zrobić, zobacz sekcję "Rejestrowanie i wyrejestrowywanie maszyn przy użyciu interfejsu wiersza polecenia" (s. 132).

Dodatkowe parametry

`--http-proxy-host=<IP address>` i `--http-proxy-port=<port>`

Serwer proxy HTTP, którego agent będzie używać do tworzenia kopii zapasowych lub odzyskiwania z chmury i nawiązywania połączenia z serwerem zarządzania. W przypadku nieokreślenia tych parametrów serwer proxy nie będzie używany.

`--http-proxy-login=<login>` i `--http-proxy-password=<password>`

Poświadczenia dostępu do serwera proxy HTTP. Jeśli serwer wymaga uwierzytelniania, należy użyć tych parametrów.

`--tmp-dir=<location>`

Umożliwia wskazanie folderu, w którym mają być przechowywane pliki tymczasowe podczas instalacji. Domyślny folder to **/var/tmp**.

`{-s|--disable-native-shared}`

Podczas instalacji będą używane biblioteki redystrybucyjne, nawet jeśli będą już dostępne w systemie.

`--skip-prereq-check`

Zostanie pominięte sprawdzenie, czy są już zainstalowane pakiety wymagane do skompilowania modułu snapapi.

`--force-weak-snapapi`

Instalator nie będzie kompilował modułu snapapi. Zamiast tego użyje gotowego modułu, który może nie pasować dokładnie do jądra systemu Linux. Odradzamy korzystanie z tej opcji.

© Acronis International GmbH, 2003-2024

`--skip-svc-start`

Usługi nie zostaną automatycznie uruchomione po instalacji. Najczęściej parametr ten jest używany z parametrem `--skip-registration`.

Parametry informacyjne

`{-?|--help}`

Umożliwia wyświetlenie opisu parametrów.

`--usage`

Umożliwia wyświetlenie krótkiego opisu zastosowań polecenia.

`{-v|--version}`

Umożliwia wyświetlenie wersji pakietu instalacyjnego.

`--product-info`

Umożliwia wyświetlenie nazwy produktu i wersji pakietu instalacyjnego.

`--snapapi-list`

Umożliwia wyświetlenie dostępnych gotowych modułów snapapi.

`--components-list`

Umożliwia wyświetlenie komponentów instalatora.

Parametry dotyczące starszych funkcji

Te parametry dotyczą starego komponentu agent.exe.

`{-e|--ssl=}<path>`

Umożliwia podanie ścieżki do niestandardowego pliku certyfikatu na potrzeby komunikacji SSL.

`{-p|--port=}<port>`

Umożliwia wskazanie portu, na którym agent.exe nasłuchuje połączeń. Portem domyślnym jest port 9876.

Parametry dezinstalacji

`{-u|--uninstall}`

Powoduje dezinstalację programu.

`--purge`

Umożliwia odinstalowanie produktu i usunięcie jego dzienników, zadań oraz ustawień konfiguracyjnych. W przypadku korzystania z parametru `--uninstall` nie trzeba jawnie określać parametru `--purge`.

© Acronis International GmbH, 2003-2024

Przykłady

- Instalowanie agenta dla systemu Linux bez rejestrowania go.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- Instalowanie agenta dla systemu Linux, agenta dla Virtuozzo i agenta dla programu Oracle oraz rejestrowanie ich przy użyciu poświadczeń.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
```

- Instalowanie agenta dla programu Oracle i agenta dla systemu Linux oraz rejestrowanie ich przy użyciu tokenu rejestracji.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- Instalowanie agenta dla systemu Linux, agenta dla Virtuozzo i agenta dla programu Oracle przy użyciu ustawień konfiguracyjnych w osobnym pliku tekstowym.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
```

- Odinstalowywanie agenta dla systemu Linux, agenta dla Virtuozzo i agenta dla programu Oracle oraz usuwanie wszystkich ich dzienników, zadań oraz ustawień konfiguracyjnych.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

Instalowanie i odinstalowywanie agentów ochrony w systemie macOS

W tej sekcji opisano, jak zainstalować i odinstalować agenta ochrony w trybie nienadzorowanym na komputerze z systemem macOS przy użyciu wiersza polecenia.

Wymagane uprawnienia

Przed zainicjowaniem instalacji nienadzorowanej na obciążeniu Mac trzeba zmodyfikować ustawienia pakietu Privacy Preferences Policy Control tak, aby zezwolić na dostęp do aplikacji oraz włączyć rozszerzenia jądra i systemu w systemie macOS obciążenia w celu umożliwienia instalacji agenta Cyber Protection. Zobacz "Uprawnienia wymagane do instalacji nienadzorowanej w systemie macOS" (s. 118).

Po wdrożeniu ładunku PPPC można wykonać poniższe procedury.

Aby pobrać plik instalacyjny (.dmg)

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij **Dodaj**, a następnie kliknij **Mac**.

Aby zainstalować agenta

1. Otwórz terminal.
2. Utwórz tymczasowy katalog, w którym zamontujesz plik instalacyjny (.dmg).

   ```
   mkdir <dmg_root>
   ```

   Tutaj `<dmg_root>` oznacza dowolną odpowiadającą Ci nazwę.
3. Zamontuj plik .dmg.

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   Tutaj `<dmg_file>` oznacza nazwę pliku instalacyjnego. Na przykład **Cyber_Protection_Agent_for_MAC_x64.dmg**.
4. Uruchom instalator.
   - Jeśli korzystasz z pełnego instalatora dla systemu Mac, takiego jak `CyberProtect_AgentForMac_x64.dmg` czy `CyberProtect_AgentForMac_arm64.dmg`, uruchom następujące polecenie.

     ```
     sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
     ```

     Uwaga
     Jeśli występuje potrzeba włączenia automatycznego wdrożenia usługi File Sync & Share, zamiast tego uruchom poniższe polecenie. Ta opcja spowoduje zapytanie o hasło administratora.

     ```
     open <dmg_root>/Install.app --args --unattended --fss-onboarding-auto-start
     ```

   - Jeśli korzystasz z uniwersalnego instalatora dla systemu Mac, takiego jak `CyberProtect_AgentForMac_web.dmg`, uruchom następujące polecenie.

     ```
     sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
     ```
5. Odmontuj plik instalacyjny (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Przykład

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint
mydirectory
```


© Acronis International GmbH, 2003-2024

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

Aby odinstalować agenta

1. Otwórz terminal.
2. Wykonaj jedną z następujących czynności:
   - Aby odinstalować agenta, uruchom następujące polecenie:

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm
     ```

   - Aby odinstalować agenta i usunąć wszystkie dzienniki, zadania oraz ustawienia konfiguracyjne, uruchom następujące polecenie:

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
     ```

Uprawnienia wymagane do instalacji nienadzorowanej w systemie macOS

Przed zainicjowaniem instalacji nienadzorowanej na obciążeniu Mac trzeba zmodyfikować ustawienia pakietu Privacy Preferences Policy Control tak, aby zezwolić na dostęp do aplikacji oraz włączyć rozszerzenia jądra i systemu w systemie macOS obciążenia w celu umożliwienia instalacji agenta Cyber Protection. Można to zrobić dzięki wdrożeniu niestandardowego ładunku PPPC lub skonfigurowaniu preferencji w graficznym interfejsie użytkownika obciążenia. Wymagane są następujące uprawnienia.

Wymagania w przypadku systemu macOS 11 (Big Sur) lub nowszego

Karta	Sekcja	Pole	Wartość

© Acronis International GmbH, 2003-2024

Privacy Preferences Policy Control	Dostęp do aplikacji	Identyfikator	com.acronis.backup

© Acronis International GmbH, 2003-2024

		Typ identyfikatora	Identyfikator pakietu

© Acronis International GmbH, 2003-2024

		Wymaganie dotyczące kodu	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APLIKACJA LUB USŁUGA	SystemPolicyAllFiles
		DOSTĘP	Pozwól
	Dostęp do aplikacji	Identyfikator	com.acronis.backup.aakore
		Typ identyfikatora	Identyfikator pakietu
		Wymaganie dotyczące kodu	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APLIKACJA LUB USŁUGA	SystemPolicyAllFiles
		DOSTĘP	Pozwól
	Dostęp do aplikacji	Zidentyfikowano	com.acronis.backup.activeprotection
		Typ identyfikatora	Identyfikator pakietu
		Wymaganie dotyczące kodu	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APLIKACJA LUB USŁUGA	SystemPolicyAllFiles
		DOSTĘP	Pozwól

© Acronis International GmbH, 2003-2024

	Dostęp do aplikacji	Identyfikator	cyber-protect-service
		Typ identyfikatora	Identyfikator pakietu
		Wymaganie dotyczące kodu	`identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		APLIKACJA LUB USŁUGA	SystemPolicyAllFiles
		DOSTĘP	Pozwól
Rozszerzenia systemu		Zezwalaj użytkownikom na zatwierdzanie rozszerzeń systemu	Włączone
	Dozwolone identyfikatory zespołu i rozszerzenia systemu	Nazwa wyświetlana	Rozszerzenia systemu agenta Acronis Cyber Protection Agent
		Typy rozszerzeń systemu	Dozwolone identyfikatory zespołu
		Identyfikator zespołu	ZU2TV78AA6

Wymagania w przypadku systemu macOS w wersjach starszych niż 11

Karta	Sekcja	Pole	Wartość

© Acronis International GmbH, 2003-2024

Privacy Preferences Policy Control	Dostęp do aplikacji	Identyfikator	com.acronis.backup

© Acronis International GmbH, 2003-2024

		Typ identyfikatora	Identyfikator pakietu

© Acronis International GmbH, 2003-2024

		Wymaganie dotyczące kodu	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APLIKACJA LUB USŁUGA	SystemPolicyAllFiles
		DOSTĘP	Pozwól
	Dostęp do aplikacji	Identyfikator	com.acronis.backup.aakore
		Typ identyfikatora	Identyfikator pakietu
		Wymaganie dotyczące kodu	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APLIKACJA LUB USŁUGA	SystemPolicyAllFiles
		DOSTĘP	Pozwól
	Dostęp do aplikacji	Zidentyfikowano	com.acronis.backup.activeprotection
		Typ identyfikatora	Identyfikator pakietu
		Wymaganie dotyczące kodu	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APLIKACJA LUB USŁUGA	SystemPolicyAllFiles
		DOSTĘP	Pozwól

© Acronis International GmbH, 2003-2024

	Dostęp do aplikacji	Identyfikator	cyber-protect-service
		Typ identyfikatora	Identyfikator pakietu
		Wymaganie dotyczące kodu	identifier "cyber-protect-service" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		APLIKACJA LUB USŁUGA	SystemPolicyAllFiles
		DOSTĘP	Pozwól
Zatwierdzone rozszerzenia jądra		Zezwalaj użytkownikom na zatwierdzanie rozszerzeń jądra	Włączone
		Zezwalaj standardowym użytkownikom na zatwierdzanie starszych rozszerzeń jądra (macOS 11 lub nowszy)	Włączone
	Zatwierdzone identyfikatory zespołów i rozszerzenia jądra	Zatwierdzony identyfikator zespołu — nazwa wyświetlana	Rozszerzenia jądra agenta Acronis Cyber Protection Agent
		Identyfikator zespołu	ZU2TV78AA6
		Identyfikatory pakietów rozszerzeń jądra	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
Rozszerzenia systemu		Zezwalaj użytkownikom na zatwierdzanie rozszerzeń systemu	Włączone
	Dozwolone identyfikatory zespołu i rozszerzenia	Nazwa wyświetlana	Rozszerzenia systemu agenta Acronis Cyber Protection Agent

© Acronis International GmbH, 2003-2024

	systemu		
		Typy rozszerzeń systemu	Dozwolone identyfikatory zespołu
		Identyfikator zespołu	ZU2TV78AA6

Rejestracja maszyn

Rejestracja spowoduje połączenie maszyny, na której jest zainstalowany agent ochrony, z kontem użytkownika w ramach dzierżawcy-klienta. Po zakończeniu rejestracji maszyna będzie widoczna w konsoli Cyber Protect, w obszarze **Urządzenia** > **Komputery z agentami**. Zarejestrowanymi maszynami można zarządzać przez stosowanie do nich planów.

W przypadku instalowania agenta ochrony przy użyciu graficznego interfejsu użytkownika rejestracja stanowi część procedury instalacji.

Korzystając z interfejsu wiersza polecenia, możesz przeprowadzić rejestrację jako autonomiczną procedurę.

Rejestrowanie maszyn przy użyciu graficznego interfejsu użytkownika

W przypadku instalowania agenta ochrony przy użyciu graficznego interfejsu użytkownika rejestracja stanowi część procedury instalacji.

Dostępne są następujące metody rejestracji:

- Rejestracja w konsoli Cyber Protect
- Rejestracja przy użyciu poświadczeń dostępu do konta użytkownika
- Rejestracja przy użyciu tokenu rejestracji

Agent zostaje automatycznie wyrejestrowany po jego odinstalowaniu.

Rejestrowanie maszyn przy użyciu konsoli Cyber Protect

Ta procedura ma zastosowanie w przypadku instalowania agenta ochrony przy użyciu domyślnych ustawień instalacji (**Ustawienia rejestracji** > **Użyj konsoli Cyber Protect**).

Aby zarejestrować maszynę z poziomu konsoli Cyber Protect

1. W kreatorze instalacji kliknij **Zarejestruj obciążenie**.
   Zostanie otwarta konsola Cyber Protect.

   Uwaga
   Nie zamykaj kreatora instalacji przed zakończeniem rejestracji. W przeciwnym razie konieczne będzie powtórzenie instalacji i ponowne rozpoczęcie rejestracji.

© Acronis International GmbH, 2003-2024

2. Zaloguj się do konsoli Cyber Protect.
3. [Jeśli logujesz się jako administrator] Na ekranie **Rejestracja obciążenia** wybierz konto, w ramach którego chcesz zarejestrować maszynę.

   Konto to musi być kontem w ramach dzierżawcy-klienta. Administratorzy partnerów mogą wyświetlać dzierżawców-klientów, którymi zarządzają, i rejestrować maszyny na kontach w ramach tych dzierżawców.
4. Kliknij **Sprawdź poprawność kodu**.
5. Kliknij **Dalej**.
6. [Nie dotyczy administratorów partnerów] Przejrzyj wstępnie wybrane plany domyślne, które zostaną zastosowane do maszyny.

   Aby uzyskać więcej informacji na temat planów domyślnych, zobacz sekcję "Plany domyślne" (s. 217).

   Ważne

   Wybrane plany zostaną zastosowane tylko do maszyn z systemem Windows.

   W przypadku maszyn z systemem Linux lub macOS zastosuj plany ręcznie po zakończeniu rejestracji.
7. [Opcjonalnie] [Nie dotyczy administratorów partnerów] Aby zmienić wcześniej wybrany plan, kliknij **Zmień**.
   - Aby zastosować inny plan, wybierz plan, którego chcesz użyć, a następnie kliknij **Zmień**.

     Możesz wybrać plan od dzierżawcy lub plan wbudowany.

     Aby uzyskać więcej informacji na temat planów wbudowanych, zobacz sekcję "Plany wbudowane" (s. 208).
   - Aby zarejestrować maszynę bez stosowania planu, wybierz **Nie stosuj planu ochrony**, a następnie kliknij **Zmień**.
8. Kliknij **Zarejestruj**.

W rezultacie maszyna zostanie zarejestrowana w ramach określonego konta użytkownika. Po zakończeniu rejestracji wybrane plany zostaną automatycznie zastosowane do maszyn z systemem Windows.

Rejestrowanie maszyn przy użyciu poświadczeń użytkownika

Możesz zmodyfikować domyślną procedurę instalacji i wybrać rejestrację przy użyciu nazwy użytkownika i hasła, a nie rejestrację w konsoli Cyber Protect.

Aby zarejestrować maszynę przy użyciu nazwy użytkownika i hasła

1. W kreatorze instalacji kliknij **Dostosuj ustawienia instalacji**.
2. W sekcji **Ustawienia rejestracji** kliknij **Zmień**.
3. Wybierz **Użyj poświadczeń**.
4. Podaj nazwę użytkownika i hasło konta, w ramach którego chcesz zarejestrować maszynę.

© Acronis International GmbH, 2003-2024

To konto musi być kontem w ramach dzierżawcy-klienta.

Uwaga
Można używać tylko kont, dla których nie włączono uwierzytelniania dwuskładnikowego.

5. Kliknij **Gotowe**, a następnie dokończ instalację.

Rejestrowanie maszyn przy użyciu tokenu rejestracji

Możesz zmodyfikować domyślną procedurę instalacji i wybrać rejestrację za pomocą tokenu rejestracji, a nie rejestrację w konsoli Cyber Protect.

Aby zarejestrować maszynę przy użyciu tokenu rejestracji

1. W kreatorze instalacji kliknij **Dostosuj ustawienia instalacji**.
2. W sekcji **Ustawienia rejestracji** kliknij **Zmień**.
3. Wybierz **Użyj tokenu rejestracji**.
4. Wprowadź token rejestracji.
5. Kliknij **Gotowe**, a następnie dokończ instalację.

Generowanie tokenu rejestracji

Token rejestracji to ciąg 12 znaków podzielonych na trzy części za pomocą dywizów (-). Token rejestracji przekazuje tożsamość użytkownika do programu instalacyjnego agenta bez zapisywania poświadczeń użytkownika w konsoli Cyber Protect. Dzięki temu użytkownik może rejestrować maszyny na swoim koncie bądź stosować plany ochrony do maszyn bez logowania się do konsoli.

Uwaga
Plany ochrony nie są automatycznie stosowane podczas rejestracji maszyny. Zastosowanie planu ochrony jest osobnym zadaniem.

Ze względów bezpieczeństwa tokeny mają ograniczony czas istnienia, który można dostosować. Domyślnie okres ten wynosi 3 dni.

Administratorzy mogą generować tokeny rejestracji dla wszystkich kont użytkowników w ramach dzierżawcy, którym zarządzają. Użytkownicy mogą generować tokeny rejestracji wyłącznie dla własnych kont.

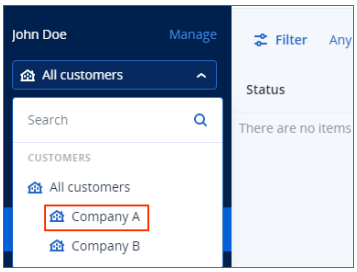
Aby wygenerować token rejestracji

Jako administrator

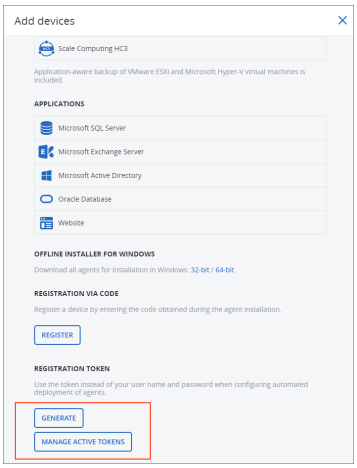
1. Zaloguj się w konsoli Cyber Protect jako administrator.
   Po zalogowaniu się do portalu zarządzania możesz przejść do konsoli Cyber Protect, klikając kolejno **Monitorowanie** > **Wykorzystanie**, a następnie kartę **Ochrona** i **Zarządzaj usługą**.

© Acronis International GmbH, 2003-2024

[W przypadku administratorów partnerów, którzy zarządzają dzierżawcami-klientami] W konsoli Cyber Protect wybierz dzierżawcę z użytkownikiem, dla którego chcesz wygenerować token. Nie można wygenerować tokenu na poziomie **Wszyscy klienci**.



2. W obszarze **Urządzenia** kliknij **Wszystkie urządzenia** > **Dodaj**.
   Z prawej strony zostanie otwarty panel **Dodaj urządzenia**.
3. Przewiń w dół do pozycji **Token rejestracji** i kliknij **Wygeneruj**.



4. Określ czas istnienia tokenu.
5. Wybierz użytkownika, dla którego chcesz wygenerować token.

> **Uwaga**
> W przypadku korzystania z tokenu obciążenia będą rejestrowane na koncie użytkownika wybranym w tym miejscu.

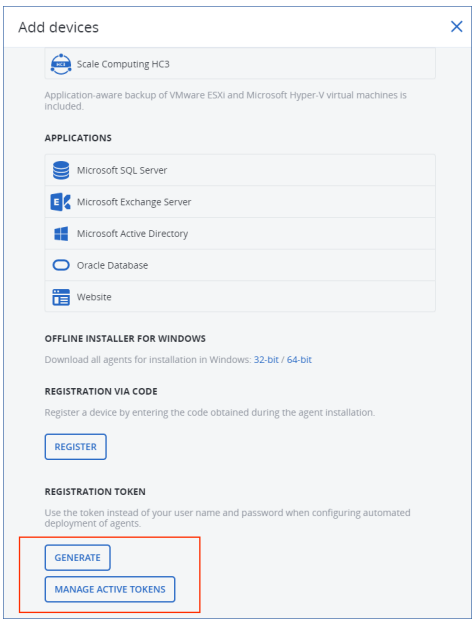
6. [Opcjonalnie] Aby umożliwić użytkownikowi tokenu stosowanie i odwoływanie planu ochrony na dodanych obciążeniach, wybierz plan z listy rozwijanej.
   Należy pamiętać, że konieczne będzie uruchomienie skryptu, który spowoduje zastosowanie lub odwołanie planu ochrony na dodanych obciążeniach. Dodatkowe informacje można znaleźć w tym artykule bazy Knowledge Base.
7. Kliknij **Wygeneruj token**.
8. Kliknij **Kopiuj**, aby skopiować token do schowka urządzenia, lub zanotuj token ręcznie.

© Acronis International GmbH, 2003-2024

Jako użytkownik

1. Zaloguj się do konsoli Cyber Protect.
2. Kliknij **Urządzenia** > **Wszystkie urządzenia** > **Dodaj**.

   Z prawej strony zostanie otwarty panel **Dodaj urządzenia**.
3. Przewiń w dół do pozycji **Token rejestracji** i kliknij **Wygeneruj**.



4. Określ czas istnienia tokenu.
5. Kliknij **Wygeneruj token**.
6. Kliknij **Kopiuj**, aby skopiować token do schowka urządzenia, lub zanotuj token ręcznie.

Zarządzanie tokenami rejestracji

Możesz przeglądać i usuwać aktywne tokeny rejestracji.

Aby wyświetlić tokeny rejestracji

1. Zaloguj się do konsoli Cyber Protect.
2. Kliknij **Urządzenia** > **Wszystkie urządzenia** > **Dodaj**.
3. Przewiń w dół do pozycji **Token rejestracji** i kliknij **Zarządzaj aktywnymi tokenami**.

   Po prawej stronie zostanie wyświetlona lista aktywnych tokenów wygenerowanych dla danego dzierżawcy.

> **Uwaga**
> Ze względów bezpieczeństwa w kolumnie **Token** będą widoczne tylko pierwsze dwa znaki wartości tokenu.

Aby usunąć token rejestracji

© Acronis International GmbH, 2003-2024

1. Zaloguj się do konsoli Cyber Protect.
2. Kliknij **Urządzenia** > **Wszystkie urządzenia** > **Dodaj**.
3. Przewiń w dół do pozycji **Token rejestracji** i kliknij **Zarządzaj aktywnymi tokenami**.
   Po prawej stronie zostanie wyświetlona lista aktywnych tokenów wygenerowanych dla danego dzierżawcy.

   Uwaga
   Ze względów bezpieczeństwa w kolumnie **Token** będą widoczne tylko pierwsze dwa znaki wartości tokenu.

4. Wybierz token, a następnie kliknij **Usuń**.

Rejestrowanie i wyrejestrowywanie maszyn przy użyciu interfejsu wiersza polecenia

Korzystając z interfejsu wiersza polecenia, możesz przeprowadzić rejestrację jako autonomiczną procedurę.

W tym przypadku nie musisz na przykład odinstalowywać agenta ochrony, jeśli chcesz go zarejestrować na innym koncie.

Rejestrowanie maszyn przy użyciu poświadczeń użytkownika

Użyj nazwy użytkownika i hasła konta, w ramach którego chcesz zarejestrować maszynę. Konto to musi być kontem w ramach dzierżawcy-klienta. Jeśli hasło zawiera znaki specjalne lub spacje, zobacz sekcję "Używanie haseł ze znakami specjalnymi lub spacjami" (s. 133).

Adres usługi to adres URL, za pomocą którego **logujesz się** do usługi Cyber Protection.

Na przykład `https://chmura.moja_firma.com.pl`.

Aby zarejestrować obciążenie z użyciem nazwy użytkownika i hasła

W systemie Windows

- W wierszu polecenia uruchom następujące polecenie:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a <service address> -u <user name> -p <password>
```

Na przykład:

© Acronis International GmbH, 2003-2024

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

W systemie Linux

- W wierszu polecenia uruchom następujące polecenie:

  ```
  sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
  <service address> -u <user name> -p <password>
  ```

Na przykład:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

W systemie macOS

Ważne
Jeśli korzystasz z systemu macOS w wersji 10.14 lub nowszej, przyznaj agentowi ochrony pełny dostęp do dysku. W tym celu przejdź do sekcji **Aplikacje** > **Narzędzia** i uruchom program **Asystent agenta Cyber Protect Agent**. Następnie postępuj zgodnie z instrukcjami wyświetlanymi w oknie aplikacji.

- W wierszu polecenia uruchom następujące polecenie:

  ```
  sudo "/Library/Application
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
  <service address> -u <user name> -p <password>
  ```

Na przykład:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

Używanie haseł ze znakami specjalnymi lub spacjami

Jeśli hasło zawiera choć jeden znak specjalny lub spację, to w przypadku wpisywania go w wierszu polecenia ujmij je w cudzysłów.

Na przykład w systemie Windows uruchom następujące polecenie:

Wzór polecenia:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <"password">
```

Przykład polecenia:

© Acronis International GmbH, 2003-2024

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

Jeśli wykonanie tego polecenia zakończy się niepowodzeniem, zakoduj hasło w formacie base64 na stronie https://www.base64encode.org/. Następnie w wierszu polecenia podaj zakodowane hasło, używając parametru -b lub --base64.

Na przykład w systemie Windows uruchom następujące polecenie:

Wzór polecenia:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -b -p <encoded password>
```

Przykład polecenia:

```
"C:\ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Rejestrowanie maszyn przy użyciu tokenu rejestracji

Token rejestracji to ciąg 12 znaków podzielonych na trzy części za pomocą dywizów (-). Token rejestracji przekazuje tożsamość użytkownika do programu instalacyjnego agenta bez zapisywania poświadczeń użytkownika w konsoli Cyber Protect. Dzięki temu użytkownik może rejestrować maszyny na swoim koncie bądź stosować plany ochrony do maszyn bez logowania się do konsoli.

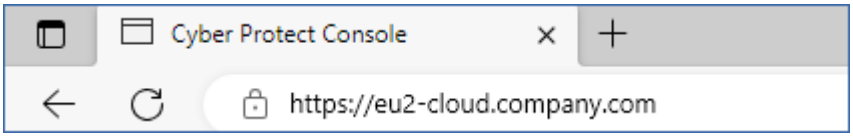
Aby uzyskać więcej informacji, zobacz "Generowanie tokenu rejestracji" (s. 129).

Uwaga
Plany ochrony nie są automatycznie stosowane podczas rejestracji maszyny. Zastosowanie planu ochrony jest osobnym zadaniem.

Więcej informacji można znaleźć w tym artykule bazy wiedzy Knowledge Base.

W przypadku korzystania z tokenu rejestracji należy podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** w usłudze Cyber Protection.

Na przykład `https://eu2-cloud.company.com`.



Aby zarejestrować obciążenie z użyciem tokenu rejestracji

W systemie Windows

© Acronis International GmbH, 2003-2024

- W wierszu polecenia uruchom następujące polecenie:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a <service address> --token <registration token>
```

Na przykład:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

W systemie Linux

- W wierszu polecenia uruchom następujące polecenie:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<service address> --token <registration token>
```

Na przykład:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

W systemie macOS

Ważne
Jeśli korzystasz z systemu macOS w wersji 10.14 lub nowszej, przyznaj agentowi ochrony pełny dostęp do dysku. W tym celu przejdź do sekcji **Aplikacje** > **Narzędzia** i uruchom program **Asystent agenta Cyber Protect Agent**. Następnie postępuj zgodnie z instrukcjami wyświetlanymi w oknie aplikacji.

- W wierszu polecenia uruchom następujące polecenie:

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<service address> --token <registration token>
```

Na przykład:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

Urządzenie wirtualne

1. W konsoli urządzenia wirtualnego naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.
2. W wierszu polecenia uruchom następujące polecenie:

```
register_agent -o register -t cloud -a <service address> --token <registration token>
```


© Acronis International GmbH, 2003-2024

Na przykład:

```
register_agent -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

3. Aby wrócić do interfejsu graficznego urządzenia, naciśnij klawisze ALT+F1.

Wyrejestrowywanie maszyn

Z poziomu interfejsu wiersza polecenia możesz wyrejestrować agenta ochrony bez jego odinstalowania.

Aby wyrejestrować obciążenie

W systemie Windows

- W wierszu polecenia uruchom następujące polecenie:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Na przykład:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

W systemie Linux

- W wierszu polecenia uruchom następujące polecenie:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

W systemie macOS

W wierszu polecenia uruchom następujące polecenie:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

Urządzenie wirtualne

1. W konsoli urządzenia wirtualnego naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.
2. W wierszu polecenia uruchom następujące polecenie:

```
register_agent -o unregister
```

3. Aby wrócić do interfejsu graficznego urządzenia, naciśnij klawisze ALT+F1.

© Acronis International GmbH, 2003-2024

Zmiana rejestracji obciążenia

Możesz zmienić bieżącą rejestrację maszyny, rejestrując ją w ramach nowego dzierżawcy lub nowego konta użytkownika.

Ważne
Gdy zmienisz rejestrację obciążenia, wszystkie plany ochrony, które są do niego przypisane, zostaną wycofane. Aby kontynuować ochronę obciążenia, zastosuj dla niego nowy plan ochrony.

Jeśli zarejestrujesz obciążenie w nowym dzierżawcy, obciążenie straci dostęp do kopii zapasowych w magazynie w chmurze pierwotnego dzierżawcy. Kopie zapasowe, które są zapisane w magazynach niebędących w chmurze, pozostaną dostępne.

Aby zmienić rejestrację obciążenia

Za pomocą interfejsu wiersza polecenia

1. Wyrejestruj agenta ochrony zgodnie z opisem: "Wyrejestrowywanie maszyn" (s. 136).
2. Zarejestruj agenta ochrony w nowym dzierżawcy albo dla nowego konta użytkownika, zgodnie z opisem: "Rejestrowanie maszyn przy użyciu poświadczeń użytkownika" (s. 132) lub "Rejestrowanie maszyn przy użyciu tokenu rejestracji" (s. 134).

Za pomocą graficznego interfejsu użytkownika

1. Odinstaluj agenta ochrony.
2. Zainstaluj agenta ochrony, a następnie zarejestruj go w nowym dzierżawcy lub dla nowego konta użytkownika.

Aby uzyskać więcej informacji na temat instalowania i rejestrowania agenta, zobacz sekcję "Instalowanie agentów ochrony przy użyciu graficznego interfejsu użytkownika" (s. 84).

Przenoszenie maszyn do innego dzierżawcy

Oprogramowanie nie zapewnia macierzystej obsługi przenoszenia obciążenia do innego dzierżawcy. Aby to obejść, można wyrejestrować obciążenie, a następnie zarejestrować je w ramach innego dzierżawcy. Wszystkie zastosowane plany ochrony zostaną odwołane z tego obciążenia i utraci ono dostęp do swoich kopii zapasowych w chmurze pierwotnego dzierżawcy.

Dokładniejsze instrukcje dotyczące rejestrowania obciążenia w ramach nowego dzierżawcy lub na nowym koncie użytkownika można znaleźć w sekcji "Zmiana rejestracji obciążenia" (s. 137).

Aktualizowanie agentów ochrony

Wszystkie agenty można aktualizować ręcznie przy użyciu konsoli Cyber Protect lub przez pobranie i uruchomienie pliku instalacyjnego.

Aktualizacje automatyczne można skonfigurować w przypadku następujących agentów:

© Acronis International GmbH, 2003-2024

- Agent dla systemu Windows
- Agent dla systemu Linux
- Agent dla systemu Mac
- Cyber Files Cloud Agent dla File Sync & Share

Do automatycznej lub ręcznej aktualizacji agenta przy użyciu konsoli Cyber Protect potrzeba 4,2 GB wolnego miejsca w następującej lokalizacji:

- W przypadku systemu Linux — katalog główny
- W przypadku systemu Windows — wolumin, na którym jest zainstalowany agent

Do aktualizacji agenta w systemie macOS potrzeba 5 GB wolnego miejsca w katalogu głównym.

Uwaga
[W przypadku wszystkich agentów dostarczanych w formie urządzenia wirtualnego, w tym agenta dla VMware, agenta dla Scale Computing, agenta dla Virtuozzo Hybrid Infrastructure, agenta dla RHV (oVirt)]

Aby przeprowadzić automatyczną lub ręczną aktualizację urządzenia wirtualnego znajdującego się za serwerem proxy, trzeba skonfigurować serwer proxy na każdym urządzeniu w niżej opisany sposób.

W pliku `/opt/acronis/etc/va-updater/config.yaml` dodaj następujący wiersz tekstu na końcu pliku, podając odpowiednie wartości dla danego środowiska:

```
httpProxy: http://proxy_login:proxy_password@proxy_address:port
```

Ręczne aktualizowanie agentów ochrony

Agenty można aktualizować za pomocą konsoli Cyber Protect lub przez pobranie i uruchomienie pliku instalacyjnego.

Urządzenia wirtualne w następujących wersjach można aktualizować tylko przy użyciu konsoli Cyber Protect:

- Agent dla VMware (urządzenie wirtualne): wersja 12.5.23094 lub nowsza.
- Agent dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne): wersja 12.5.23094 lub nowsza.

Przy użyciu konsoli Cyber Protect można też aktualizować agenty w następujących wersjach:

- Agent dla systemu Windows, agent dla VMware (Windows), agent dla Hyper-V: wersja 12.5.21670 lub nowsza.
- Agent dla systemu Linux: wersja 12.5.23094 lub nowsza.
- Inne agenty: wersja 12.5.23094 lub nowsza.

Aby sprawdzić wersję agenta, w konsoli Cyber Protect wybierz komputer, a następnie kliknij **Szczegóły**.

© Acronis International GmbH, 2003-2024

Aby zaktualizować starsze wersje tych agentów, pobierz najnowszą wersję i zainstaluj ją ręcznie. Aby znaleźć łącza pobierania, kliknij **Wszystkie urządzenia** > **Dodaj**.

Wymagania wstępne

Na komputerach z systemem Windows funkcje usługi Cyber Protect wymagają pakietu redystrybucyjnego Microsoft Visual C++ 2017. Sprawdź, czy jest on już zainstalowany na komputerze, i ewentualnie go zainstaluj przed zaktualizowaniem agenta. Po zainstalowaniu pakietu może być wymagane ponowne uruchomienie komputera. Pakiet redystrybucyjny Microsoft Visual C++ jest dostępny w witrynie internetowej firmy Microsoft: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Aby zaktualizować agenta przy użyciu konsoli Cyber Protect

1. Kliknij **Ustawienia** > **Agenty**.
   W oprogramowaniu zostanie wyświetlona lista komputerów. Komputery z nieaktualnymi wersjami agentów są oznaczone pomarańczowym wykrzyknikiem.
2. Wybierz komputery, na których chcesz zaktualizować agenty. Komputery te muszą być w trybie online.
3. Kliknij **Aktualizuj agenta**.

Uwaga
Podczas aktualizacji wszelkie trwające operacje tworzenia kopii zapasowych zakończą się niepowodzeniem.

Aby zaktualizować agenta dla VMware (urządzenie wirtualne) w wersji starszej niż 12.5.23094

1. Kliknij **Ustawienia** > **Agenci** > agent do zaktualizowania > **Szczegóły** i przyjrzyj się ustawieniom w sekcji **Przypisane maszyny wirtualne**. Po aktualizacji trzeba będzie te ustawienia ponownie wprowadzić.
   a. Zwróć uwagę na położenie przełącznika **Przypisanie automatyczne**.
   b. Aby sprawdzić, które maszyny wirtualne zostały ręcznie przypisane do agenta, kliknij łącze **Przypisane**. W oprogramowaniu zostanie wyświetlona lista przypisanych maszyn wirtualnych. Zwróć uwagę na maszyny z oznaczeniem `(M)` po nazwie agenta w kolumnie **Agent**.
2. Usuń agenta dla VMware (urządzenie wirtualne) zgodnie z opisem podanym w sekcji „Odinstalowywanie agentów”. W kroku 5 usuń agenta z obszaru **Ustawienia** > **Agenty**, nawet jeśli planujesz go ponownie zainstalować.
3. Wdróż agenta dla VMware (urządzenie wirtualne) zgodnie z opisem podanym w sekcji „Wdrażanie szablonu OVF”.
4. Skonfiguruj agenta dla VMware (urządzenie wirtualne) zgodnie z opisem podanym w sekcji „Konfigurowanie urządzenia wirtualnego”.
   Jeśli chcesz odtworzyć magazyn podłączony lokalnie, w kroku 7 zrób tak:

© Acronis International GmbH, 2003-2024

a. Dodaj dysk z magazynem lokalnym do urządzenia wirtualnego.

b. Kliknij **Odśwież** > **Utwórz magazyn** > **Zamontuj**.

c. W oprogramowaniu zostanie wyświetlona oryginalna **Litera** i **Etykieta** dysku. Pozostaw je bez zmian.

d. Kliknij **OK**.

5. Kliknij **Ustawienia** > **Agenci** > agent do zaktualizowania > **Szczegóły** i odtwórz ustawienia zapamiętane w kroku 1. Jeśli niektóre maszyny wirtualne zostały ręcznie przypisane do agenta, przypisz je ponownie, tak jak opisano w sekcji „Wiązanie maszyn wirtualnych”.

   Po ukończeniu konfiguracji agenta plany ochrony, które zostały zastosowane do starego agenta, zostaną automatycznie ponownie zastosowane do nowego agenta.
6. Plany z włączoną funkcją tworzenia kopii zapasowych uwzględniających aplikacje wymagają ponownego wprowadzenia poświadczeń dostępu do systemu operacyjnego-gościa. Edytuj te plany i ponownie wprowadź poświadczenia.
7. Plany obejmujące tworzenie kopii zapasowej konfiguracji ESXi wymagają ponownego wprowadzenia hasła użytkownika „root”. Edytuj te plany i ponownie wprowadź hasło.

Aby zaktualizować definicje cyberochrony na komputerze

1. Kliknij **Ustawienia** > **Agenty**.
2. Wybierz komputer, na którym chcesz zaktualizować definicje cyberochrony, i kliknij **Aktualizuj definicje**. Komputery te muszą być w trybie online.

Aby przypisać rolę aktualizatora do agenta

1. Kliknij **Ustawienia** > **Agenty**.
2. Wybierz komputer, do którego chcesz przypisać rolę aktualizatora, kliknij **Szczegóły**, a następnie w sekcji **Definicje cyberochrony** zaznacz **Użyj tego agenta, aby pobrać oraz rozpowszechnić poprawki i aktualizacje**.

Uwaga
Agent mający rolę Aktualizator może pobierać i dystrybuować poprawki tylko w przypadku produktów innych firm przeznaczonych dla systemu Windows. W przypadku produktów firmy Microsoft dystrybucja poprawek nie jest obsługiwana przez agenta z rolą Aktualizator.

Aby wyczyścić dane z pamięci podręcznej agenta

1. Kliknij **Ustawienia** > **Agenty**.
2. Wybierz komputer, na którym chcesz wyczyścić dane z pamięci podręcznej (przestarzałe pliki aktualizacji i dane zarządzania poprawkami), i kliknij **Wyczyść pamięć podręczną**.

Automatyczne aktualizowanie agentów ochrony

Aby ułatwić zarządzanie wieloma obciążeniami, można skonfigurować automatyczne aktualizacje agenta dla systemu Windows, agenta dla systemu Linux i agenta dla systemu Mac. Aktualizacje

 © Acronis International GmbH, 2003-2024

automatyczne są dostępne w przypadku agentów w wersji 15.0.26986 (wydanej w maju 2021 r.) lub nowszej. Starsze agenty trzeba najpierw ręcznie zaktualizować do najnowszej wersji.

Aktualizacje automatyczne są obsługiwane na komputerach z dowolnym z następujących systemów operacyjnych:

- Windows XP SP 3 i nowsze wersje
- Red Hat Enterprise Linux 6 i nowsze wersje, CentOS 6 i nowsze wersje
- OS X 10.9 Mavericks i nowsze wersje

Ustawienia aktualizacji automatycznych są wstępnie skonfigurowane na poziomie centrum danych. Administrator firmy może je dostosować — dla wszystkich komputerów w firmie lub jednostce albo tylko dla wybranych komputerów. Jeśli nie są stosowane żadne ustawienia niestandardowe, używane są ustawienia z wyższego poziomu, w następującej kolejności:

1. Centrum danych Cyber Protection
2. Firma (dzierżawca-klient)
3. Jednostka
4. Komputer

Na przykład administrator jednostki może skonfigurować dla wszystkich komputerów w jednostce niestandardowe ustawienia aktualizacji automatycznych, które mogą się różnić od ustawień zastosowanych do komputerów na poziomie firmy. Administrator może też skonfigurować inne ustawienia dla jednego lub kilku komputerów w jednostce, do których nie zostaną zastosowane ani ustawienia jednostki, ani ustawienia firmy.

Po włączeniu aktualizacji automatycznych można skonfigurować następujące opcje:

- **Kanał aktualizacji**

  Kanał aktualizacji określa, która wersja agentów zostanie użyta — najbardziej aktualna czy najnowsza wersja z poprzedniego wydania.
- **Okno na konserwację**

  Okno na konserwację określa, kiedy mogą być instalowane aktualizacje. W przypadku wyłączenia opcji okna na konserwację aktualizacje mogą być uruchamiane w dowolnym czasie.

  Aktualizacje nie będą instalowane nawet w ramach włączonego okna na konserwację, jeśli agent wykonuje którąkolwiek z poniższych operacji:
  - Kopia zapasowa
  - Odzyskiwanie
  - Replikacja kopii zapasowej
  - Replikacja maszyn wirtualnych
  - Testowanie repliki
  - Uruchamianie maszyny wirtualnej z kopii zapasowej (łącznie z finalizacją)
  - Przełączanie awaryjne w ramach odzyskiwania po awarii

© Acronis International GmbH, 2003-2024

- Powrót po awarii w ramach odzyskiwania po awarii
- Uruchamianie skryptu (w przypadku funkcji Obsługa skryptów cybernetycznych)
- Instalacja poprawek
- Kopia zapasowa konfiguracji hosta ESXi

Aby dostosować ustawienia aktualizacji automatycznych

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Wybierz zakres ustawień:
   - Aby zmienić ustawienia dla wszystkich komputerów, kliknij **Edytuj domyślne ustawienia aktualizacji agentów**.
   - Aby zmienić ustawienia dla wybranych komputerów, wybierz te komputery, a następnie kliknij **Ustawienia aktualizacji agentów**.
3. Skonfiguruj ustawienia stosownie do swoich potrzeb, a następnie kliknij **Zastosuj**.

Aby usunąć niestandardowe ustawienia aktualizacji automatycznych

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Wybierz zakres ustawień:
   - Aby usunąć niestandardowe ustawienia dla wszystkich komputerów, kliknij **Edytuj domyślne ustawienia aktualizacji agentów**.
   - Aby usunąć niestandardowe ustawienia dla wybranych komputerów, wybierz te komputery, a następnie kliknij **Ustawienia aktualizacji agentów**.
3. Kliknij **Resetuj do ustawień domyślnych**, a następnie kliknij **Zastosuj**.

Aby sprawdzić status aktualizacji automatycznych

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Kliknij ikonę koła zębatego w prawym górnym rogu tabeli i dopilnuj, aby było zaznaczone pole wyboru **System**.
3. Sprawdź status wyświetlany w kolumnie **Aktualizuj automatycznie**.

Aktualizowanie agentów ochrony na maszynach zaszyfrowanych przy użyciu funkcji BitLocker

Aktualizacje agenta, które wprowadzają zmiany w narzędziu Startup Recovery Manager, zakłócają działanie funkcji BitLocker na obciążeniach, na których włączono zarówno funkcję BitLocker, jak i narzędzie Startup Recovery Manager. W takim przypadku po ponownym uruchomieniu wymagany jest klucz odzyskiwania funkcji BitLocker. Aby ograniczyć skutki tego problemu, należy zawiesić lub wyłączyć funkcję BitLocker przed rozpoczęciem aktualizacji agenta.

Wersje agenta, których to dotyczy:

© Acronis International GmbH, 2003-2024

- 23.12.36943, wydany w grudniu 2023

W informacjach o wersji agenta ochrony można też sprawdzić, czy aktualizacja wprowadza zmiany w narzędziu Startup Recovery Manager.

Aby zaktualizować agenta na obciążeniu, na którym włączono funkcję BitLocker i narzędzie Startup Recovery Manager

1. Na obciążeniu, na którym chcesz zaktualizować agenta, zawieś lub wyłącz funkcję BitLocker.
2. Zaktualizuj agenta.
3. Uruchom ponownie obciążenie.
4. Włącz funkcję BitLocker.

Wdrażanie agentów ochrony przy użyciu zasad grupy

Agenta dla systemu Windows można centralnie zainstalować (lub wdrożyć) na komputerach należących do domeny Active Directory, korzystając z zasad grupy systemu Windows.

W tej sekcji przedstawiono sposób konfigurowania obiektu zasad grupy w celu wdrożenia agentów na komputerach w całej domenie lub jej jednostce organizacyjnej.

Za każdym razem, gdy komputer loguje się do domeny, wynikowy obiekt zasad grupy sprawdza, czy agent jest zainstalowany i zarejestrowany.

Wymagania wstępne

- Domena Active Directory z kontrolerem domeny, na którym działa system Microsoft Windows Server 2003 lub nowszy.
- Należysz do grupy **Administratorzy domeny** w domenie.
- Masz pobrany program instalacyjny **Wszystkie agenty dla systemu Windows**.
  Aby pobrać program instalacyjny, w konsoli Cyber Protect kliknij ikonę konta widoczną w prawym górnym rogu, a następnie kliknij **Do pobrania**. Łącze pobierania jest też dostępne w panelu **Dodaj urządzenia**.

Aby wdrożyć agenty przy użyciu zasad grupy

1. Wygeneruj token rejestracji zgodnie z opisem podanym w sekcji "Generowanie tokenu rejestracji" (s. 129).
2. Utwórz pliki .mst, .msi i .cab zgodnie z opisem podanym w sekcji "Tworzenie pliku transformacji i wyodrębnianie pakietów instalacyjnych" (s. 144).
3. Skonfiguruj obiekt zasad grupy zgodnie z opisem podanym w sekcji "Konfigurowanie obiektu zasad grupy" (s. 144).

© Acronis International GmbH, 2003-2024

Tworzenie pliku transformacji i wyodrębnianie pakietów instalacyjnych

Aby wdrożyć agenty ochrony za pomocą zasad grupy systemu Windows, potrzebny jest plik transformacji (.mst) oraz pakiety instalacyjne (pliki .msi i .cab).

Uwaga
Na potrzeby poniższej procedury wykorzystano domyślną opcję rejestracji, czyli rejestrację przy użyciu tokenu. Instrukcję generowania tokenu rejestracji można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129).

Aby utworzyć plik .mst i wyodrębnić pakiety instalacyjne (pliki .msi i .cab)

1. Zaloguj się jako administrator na dowolnym komputerze w domenie Active Directory.
2. Utwórz folder udostępniony, w którym będą przechowywane pakiety instalacyjne. Upewnij się, że użytkownicy domeny mają dostęp do tego folderu udostępnionego — w tym celu na przykład pozostaw domyślne ustawienia udostępniania dla opcji **Wszyscy**.
3. Uruchom program instalacyjny agenta.
4. Kliknij **Utwórz pliki .mst i .msi na potrzeby instalacji nienadzorowanej**.
5. W polu **Elementy do zainstalowania** wybierz komponenty, które mają zostać uwzględnione w instalacji, a następnie kliknij **Gotowe**.
6. W polu **Ustawienia rejestracji** kliknij **Określ**, wpisz token rejestracji, a następnie kliknij **Gotowe**. Możesz zmienić metodę rejestracji z **Użyj tokenu rejestracji** (opcja domyślna) na **Użyj poświadczeń** lub **Pomiń rejestrację**. Wybór opcji **Pomiń rejestrację** jest dokonywany przy założeniu późniejszej ręcznej rejestracji obciążeń.
7. Przejrzyj lub zmodyfikuj ustawienia instalacji, które zostaną dodane do pliku .mst, a następnie kliknij **Kontynuuj**.
8. W polu **Zapisz pliki w** podaj ścieżkę do utworzonego udostępnionego folderu.
9. Kliknij **Wygeneruj**.

W wyniku tego pliki .mst, .msi i .cab zostaną utworzone oraz skopiowane do wskazanego udostępnionego folderu.

Następnie skonfiguruj obiekt zasad grupy systemu Windows. Aby się dowiedzieć, jak to zrobić, zapoznaj się z sekcją "Konfigurowanie obiektu zasad grupy" (s. 144).

Konfigurowanie obiektu zasad grupy

W tej procedurze używane są pakiety instalacyjne utworzone w ramach sekcji "Tworzenie pliku transformacji i wyodrębnianie pakietów instalacyjnych" (s. 144) w celu skonfigurowania obiektu zasad grupy. Obiekt zasad grupy wdroży agenty na komputerach w domenie.

Aby skonfigurować obiekt zasad grupy

© Acronis International GmbH, 2003-2024

1. Zaloguj się na kontrolerze domeny jako administrator domeny.

   Jeśli domena ma więcej niż jeden kontroler, zaloguj się na dowolnym z nich jako administrator domeny.
2. [W przypadku wdrażania agentów w jednostce organizacyjnej] Upewnij się, że jednostka organizacyjna, w której chcesz wdrożyć agenty, znajduje się w ramach tej domeny.
3. W menu **Start** systemu Windows wskaż **Narzędzia administracyjne**, a następnie kliknij **Zarządzanie zasadami grupy** (lub **Użytkownicy i komputery usługi Active Directory** w przypadku systemu Windows Server 2003).
4. [W przypadku systemu Windows Server 2008 lub nowszego] Kliknij prawym przyciskiem myszy nazwę domeny lub jednostki organizacyjnej, a następnie kliknij **Utwórz obiekt zasad grupy w tej domenie i umieść tu łącze**.
5. [W przypadku systemu Windows Server 2003] Kliknij prawym przyciskiem myszy domenę lub jednostkę organizacyjną, a następnie kliknij **Właściwości**. W oknie dialogowym kliknij kartę **Zasady grupy**, a następnie kliknij **Nowy**.
6. Nadaj nazwę nowemu obiektowi zasad grupy **Agent dla systemu Windows**.
7. Otwórz obiekt zasad grupy **Agent dla systemu Windows** do edycji:
   - [W przypadku systemu Windows Server 2008 lub nowszego] W obszarze **Obiekty zasad grupy** kliknij prawym przyciskiem myszy obiekt zasad grupy, a następnie kliknij **Edytuj**.
   - [W przypadku systemu Windows Server 2003] Kliknij obiekt zasad grupy, a następnie kliknij **Edytuj**.
8. W przystawce Edytor obiektów zasad grupy rozwiń węzeł **Konfiguracja komputera**.
9. [W przypadku systemu Windows Server 2012 lub nowszego] Rozwiń węzły **Zasady** > **Ustawienia oprogramowania**.
10. [W przypadku systemów Windows Server 2003 i Windows Server 2008] Rozwiń węzeł **Ustawienia oprogramowania**.
11. Kliknij prawym przyciskiem myszy **Instalacja oprogramowania**, wskaż **Nowy**, a następnie kliknij **Pakiet**.
12. Wybierz pakiet instalacyjny .msi agenta w utworzonym przez siebie folderze udostępnionym, a następnie kliknij **Otwórz**.
13. W oknie dialogowym **Rozmieszczanie oprogramowania** kliknij **Zaawansowane**, a następnie kliknij **OK**.
14. Na karcie **Modyfikacje** kliknij **Dodaj**, a następnie wybierz plik .mst w utworzonym przez siebie folderze udostępnionym.
15. Kliknij **OK**, aby zamknąć okno dialogowe **Rozmieszczanie oprogramowania**.

© Acronis International GmbH, 2003-2024

Wdrażanie urządzeń wirtualnych

Wdrażanie agenta dla VMware (urządzenie wirtualne)

Zanim zaczniesz

Wymagania systemowe agenta

Domyślnie urządzeniu wirtualnemu przydzielane jest 4 GB pamięci RAM oraz dwa procesory vCPU, co jest optymalne i wystarczające dla większości operacji.

Aby poprawić wydajność tworzenia kopii zapasowych i uniknąć błędów związanych ze zbyt małą ilością pamięci RAM, w bardziej wymagających przypadkach zalecamy zwiększenie tych zasobów do 16 GB pamięci RAM i 4 procesorów wirtualnych. Na przykład zwiększ przypisane zasoby, jeśli się spodziewasz, że ruch związany z tworzeniem kopii zapasowych przekroczy 100 MB na sekundę (na przykład w sieciach 10-gigabitowych), lub gdy tworzysz kopię zapasową kilku maszyn wirtualnych z dużymi dyskami twardymi (500 GB lub więcej) naraz.

Własne dyski wirtualne urządzenia zajmują nie więcej niż 6 GB. Format dysku („gruby” czy „chudy”) nie ma wpływu na wydajność urządzenia.

Ile agentów potrzebuję?

Mimo iż jedno urządzenie wirtualne jest w stanie chronić całe środowisko vSphere, najlepsza praktyka zakłada użycie jednego urządzenia wirtualnego na każdy klaster vSphere (lub hosta w przypadku braku klastrów). Pozwala to na szybsze tworzenie kopii zapasowych, ponieważ urządzenie może podłączyć dyski uwzględniane w kopiach zapasowych przy użyciu transportu HotAdd, w związku z czym ruch związany z tworzeniem kopii zapasowych jest kierowany z jednego dysku lokalnego na drugi.

Normalną praktyką jest jednoczesne korzystanie z urządzenia wirtualnego i Agent dla VMware (Windows), o ile są one podłączone do tego samego serwer vCenter *lub* do innych hostów ESXi. Należy unikać sytuacji, w której jeden agent podłączony jest bezpośrednio do ESXi, a drugi agent jest podłączony do serwera vCenter zarządzającego tym ESXi.

W przypadku korzystania z więcej niż jednego agenta lepiej nie korzystać z pamięci masowej podłączonej lokalnie (tj. przechowywania kopii zapasowych na dyskach wirtualnych dodanych do urządzenia wirtualnego). Dodatkowe kwestie do uwzględnienia można znaleźć w sekcji "Używanie magazynu dołączonego lokalnie" (s. 738).

Wyłączanie automatycznego harmonogramu zasobów rozproszonych (Distributed Resource Scheduler —DRS) dla agenta

Jeśli w klastrze vSphere zostało wdrożone urządzenie wirtualne, należy wyłączyć dla niego automatyczne narzędzie vMotion. W ustawieniach DRS klastra włącz poziomy automatyzacji

© Acronis International GmbH, 2003-2024

konkretnej maszyny wirtualnej, a następnie ustaw **Poziom automatyzacji** dla urządzenia wirtualnego jako **Wyłączony**.

Wdrażanie szablonu OVF

1. Kliknij **Wszystkie urządzenia** > **Dodaj** > **VMware ESXi** > **Urządzenie wirtualne (OVF)**.
   Na Twoją maszynę zostanie pobrane archiwum zip.
2. Rozpakuj archiwum .zip. Folder ten zawiera jeden plik .ovf i dwa pliki .vmdk.
3. Dopilnuj, aby do tych plików można było uzyskać dostęp z komputera z klientem vSphere.
4. Uruchom klienta vSphere i zaloguj się na serwerze vCenter.
5. Wdróż szablon OVF.
   - Przy konfiguracji magazynu danych wybierz współdzielony magazyn danych, jeśli taki istnieje. Format dysku („gruby" czy „chudy") nie ma wpływu na wydajność urządzenia.
   - Konfigurując połączenia sieciowe, wybierz sieć, która umożliwia połączenie z Internetem, tak aby agent mógł poprawnie zarejestrować się w chmurze.

Konfigurowanie urządzenia wirtualnego

Po wdrożeniu urządzenia wirtualnego trzeba je skonfigurować tak, aby miało dostęp zarówno do serwera vCenter lub hosta ESXi, jak i do usługi Cyber Protection.

Aby skonfigurować urządzenie wirtualne

1. W kliencie vSphere otwórz konsolę urządzenia wirtualnego.
2. Upewnij się, że jest skonfigurowane połączenie sieciowe.
   Połączenie jest konfigurowane automatycznie przy użyciu protokołu DHCP (Dynamic Host Configuration Protocol).
   Aby zmienić konfigurację domyślną, w sekcji **Opcje agenta** w polu **eth0** kliknij **Zmień**, a następnie określ ustawienia sieciowe.
3. Podłącz urządzenie wirtualne do serwera vCenter lub hosta ESXi.
   a. W sekcji **Opcje agenta** w polu **vCenter/ESX(i)** kliknij **Zmień**, a następnie określ następujące opcje.
      - [Jeśli korzystasz z serwera vCenter] Nazwa lub adres IP serwera vCenter.
      - [Jeśli nie korzystasz z serwera vCenter] Nazwa lub adres IP hosta ESX, na którym chcesz tworzyć kopie zapasowe maszyn wirtualnych i je odzyskiwać. Jeśli chcesz przyspieszyć tworzenie kopii zapasowych, wdróż urządzenie wirtualne na tym samym hoście.
      - Poświadczenia wymagane do podłączenia urządzenia wirtualnego do serwera vCenter lub hosta ESXi.
        W celu uzyskania dostępu do serwera vCenter lub hosta ESXi warto korzystać ze specjalnego konta, a nie z już istniejącego konta z rolą Administrator. Dodatkowe informacje można znaleźć w sekcji "Wymagane uprawnienia dla agenta dla VMware" (s. 744).

© Acronis International GmbH, 2003-2024

b. Kliknij **Sprawdź połączenie**, aby sprawdzić poprawność ustawień.

c. Kliknij **OK**.

4. Zarejestruj urządzenie w usłudze Cyber Protection przy użyciu jednej z następujących metod.

   - [Tylko w przypadku dzierżawców, którzy nie stosują uwierzytelniania dwuskładnikowego] Zarejestruj urządzenie wirtualne w jego interfejsie graficznym.

     a. W obszarze **Opcje agenta**, w polu **Serwer zarządzania** kliknij **Zmień**.

     b. W polu **Nazwa / adres IP serwera** wybierz **Chmura**.

     Pojawi się adres usługi Cyber Protection. Nie zmieniaj tego adresu, chyba że otrzymasz inne instrukcje.

     c. W polach **Nazwa użytkownika** i **Hasło** podaj poświadczenia dostępu do konta w usłudze Cyber Protection. Na tym koncie są rejestrowane urządzenie wirtualne i maszyny wirtualne, którymi ono zarządza.

     d. Kliknij **OK**.

   - Zarejestruj urządzenie w interfejsie wiersza polecenia.

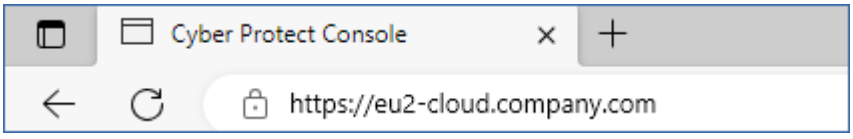
     Uwaga
     W przypadku korzystania z tej metody potrzebny jest token rejestracji. Więcej informacji o procedurze generowania tokenu można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129).

     a. Naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.

     b. Uruchom następujące polecenie:

     ```
     register_agent -o register -t cloud -a <service address> --token <registration token>
     ```

     Uwaga
     W przypadku używania tokenu rejestracji trzeba podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do konsoli Cyber Protect. Na przykład `https://eu2-cloud.company.com`.

     W tym przypadku nie używaj `https://cloud.company.com`.

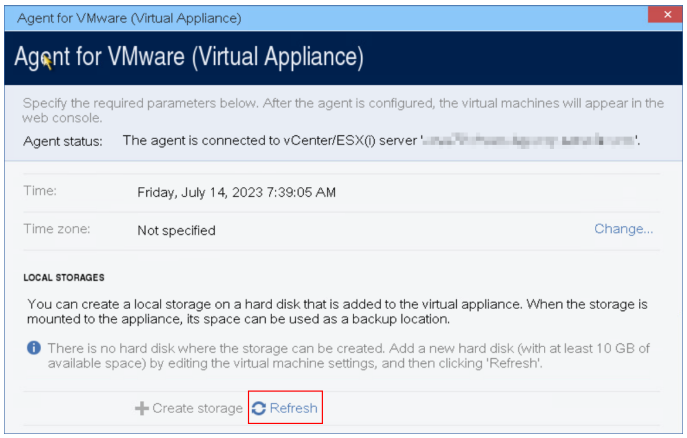
     c. Aby wrócić do interfejsu graficznego urządzenia, naciśnij klawisze ALT+F1.

5. [Opcjonalnie] Dodaj magazyn lokalny.

   a. W kliencie vSphere podłącz dysk wirtualny do urządzenia wirtualnego. Dysk wirtualny musi mieć co najmniej 10 GB wolnego miejsca.

   b. W graficznym interfejsie użytkownika urządzenia wirtualnego kliknij **Odśwież**.

© Acronis International GmbH, 2003-2024



Zostanie uaktywniony przycisk **Utwórz magazyn**.

c. Kliknij **Utwórz magazyn**.

d. Określ etykietę magazynu, a następnie kliknij **OK**.

e. Potwierdź wybór, klikając **Tak**.

6. [Jeśli w sieci jest włączony serwer proxy] Skonfiguruj serwer proxy.

a. Naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.

b. Otwórz plik **/etc/Acronis/Global.config** w edytorze tekstowym.

c. Wykonaj jedną z następujących czynności:

- Jeśli ustawienia serwera proxy zostały określone podczas instalacji agenta, znajdź następującą sekcję:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- W przeciwnym wypadku skopiuj powyższe wiersze i wklej je do pliku między znacznikami `<registry name="Global">...</registry>`.

d. Zastąp wartość `ADDRESS` nową nazwą hosta / adresem IP serwera proxy, a wartość `PORT` — wartością dziesiętną numeru portu.

e. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `LOGIN` i `PASSWORD` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.

f. Zapisz plik.

g. Otwórz plik **/opt/acronis/etc/aakore.yaml** w edytorze tekstów.

h. Znajdź sekcję **env** lub ją utwórz i dodaj następujące wiersze:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```


© Acronis International GmbH, 2003-2024

i. Zastąp zmienne `proxy_login` i `proxy_password` poświadczeniami dostępu do serwera proxy, a zmienną `proxy_address:port` — adresem i numerem portu serwera proxy.
j. Uruchom polecenie `reboot`.

Uwaga
Aby móc zaktualizować urządzenie wirtualne wdrożone za serwerem proxy, edytuj plik `config.yaml` urządzenia (`/opt/acronis/etc/va-updater/config.yaml`), dodając następujący wiersz u dołu tego pliku, a następnie wprowadzając wartości specyficzne dla danego środowiska:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Na przykład:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Wdrażanie agenta dla Scale Computing HC3 (urządzenie wirtualne)

Zanim zaczniesz

Urządzenie to jest prekonfigurowaną maszyną wirtualną, którą użytkownik wdraża w klastrze Scale Computing HC3. Zawiera ono agenta ochrony, który pozwala na administrowanie cyberochroną wszystkich maszyn wirtualnych w klastrze.

Wymagania systemowe agenta

Domyślnie maszyna wirtualna z agentem używa 2 procesorów vCPU i 4 GiB pamięci RAM. Ustawienia te są wystarczające w przypadku większości operacji, ale można je zmienić przez edycję maszyny wirtualnej w interfejsie internetowym Scale Computing HC3.

Aby poprawić wydajność tworzenia kopii zapasowych i uniknąć błędów związanych ze zbyt małą ilością pamięci RAM, w bardziej wymagających przypadkach zalecamy zwiększenie tych zasobów do 4 procesorów wirtualnych i 8 GiB pamięci RAM. Na przykład zwiększ przypisane zasoby, jeśli się spodziewasz, że ruch związany z tworzeniem kopii zapasowych przekroczy 100 MB na sekundę (na przykład w sieciach 10-gigabitowych), lub gdy tworzysz kopię zapasową kilku maszyn wirtualnych z dużymi dyskami twardymi (500 GB lub więcej) naraz.

Dysk wirtualny urządzenia ma rozmiar około 9 GB.

Ile agentów potrzebuję?

Jeden agent może chronić cały klaster. Jeśli jednak trzeba rozłożyć obciążenie sieci ruchem związanym z tworzeniem kopii zapasowych, można mieć więcej niż jednego agenta w klastrze.

W przypadku dostępności więcej niż jednego agenta w klastrze maszyny wirtualne są automatycznie przydzielane agentom, tak aby każdy z nich zarządzał podobną liczbą maszyn.

Za każdym razem, gdy różnica obciążenia między agentami przekracza 20 procent, następuje ponowny automatyczny przydział. Może się tak zdarzyć po dodaniu bądź usunięciu jednego z

© Acronis International GmbH, 2003-2024

komputerów lub agentów. Przykład: zauważasz potrzebę podłączenia większej liczby agentów w celu zwiększenia przepustowości i wdrażasz w klastrze dodatkowe urządzenie wirtualne. Serwer zarządzania przypisze najbardziej odpowiednie maszyny nowemu agentowi. Zmniejszy się obciążenie starszych agentów. W przypadku usunięcia agenta z serwera zarządzania komputery przydzielone do tego agenta zostaną ponownie przydzielone pozostałym agentom. Nie jest to jednak możliwe w przypadku uszkodzenia agenta lub jego ręcznego usunięcia z klastra Scale Computing HC3. Proces ponownego przydzielania rozpocznie się dopiero po usunięciu takiego agenta z konsoli Cyber Protect.

Aby sprawdzić, który agent zarządza danym komputerem

1. W konsoli Cyber Protect kliknij **Urządzenia**, a następnie wybierz **Scale Computing**.
2. Kliknij ikonę koła zębatego w prawym górnym rogu tabeli i w obszarze **System** zaznacz pole wyboru **Agent**.
3. Sprawdź nazwę agenta w wyświetlonej kolumnie.

Wdrażanie szablonu QCOW2

1. Zaloguj się na koncie Cyber Protection.
2. Kliknij **Urządzenia** > **Wszystkie urządzenia** > **Dodaj** > **Scale Computing HC3**.
   Na Twoją maszynę zostanie pobrane archiwum zip.
3. Rozpakuj archiwum .zip i zapisz plik .qcow2 oraz plik .xml w folderze o nazwie **ScaleAppliance**.
4. Prześlij folder **ScaleAppliance** do udziału sieciowego i upewnij się, że klaster Scale Computing HC3 ma do niego dostęp.
5. Zaloguj się do klastra Scale Computing HC3 jako administrator z przypisaną rolą **Tworzenie/edycja maszyn wirtualnych**. Dodatkowe informacje na temat ról wymaganych do operacji dotyczących maszyn wirtualnych Scale Computing HC3 można znaleźć w sekcji "Agent dla Scale Computing HC3 (urządzenie wirtualne) — wymagane role" (s. 154).
6. W interfejsie internetowym Scale Computing HC3 zaimportuj szablon maszyny wirtualnej z folderu **ScaleAppliance**.
   a. Kliknij ikonę **Import HC3 VM** (Importuj maszynę wirtualną HC3).
   b. W oknie **Import HC3 VM** (Importuj maszynę wirtualną HC3) podaj następujące informacje:
      - Nazwa nowej maszyny wirtualnej.
      - Udział sieciowy, w którym znajduje się folder **ScaleAppliance**.
      - Nazwa użytkownika i hasło wymagane w celu uzyskania dostępu do tego udziału sieciowego.
      - [Opcjonalnie] Znacznik domeny dla nowej maszyny wirtualnej.
      - Ścieżka do folderu **ScaleAppliance** w udziale sieciowym.
   c. Kliknij **Import** (Importuj).

© Acronis International GmbH, 2003-2024

Po zakończeniu wdrożenia trzeba skonfigurować urządzenie wirtualne. Dodatkowe informacje na temat jego konfigurowania można znaleźć w sekcji "Konfigurowanie urządzenia wirtualnego" (s. 152).

Uwaga
Jeśli w klastrze jest potrzebne więcej niż jedno urządzenie wirtualne, powtórz powyższe kroki i wdróż dodatkowe urządzenia. Nie klonuj istniejącego już urządzenia wirtualnego przy użyciu opcji **Clone VM** (Klonuj maszynę wirtualną) w interfejsie internetowym Scale Computing HC3.

Konfigurowanie urządzenia wirtualnego

Po wdrożeniu urządzenia wirtualnego należy je skonfigurować tak, aby miało dostęp zarówno do klastra Scale Computing HC3, który ma ono chronić, jak i do usługi Cyber Protection.

Aby skonfigurować urządzenie wirtualne

1. Zaloguj się na koncie Scale Computing HC3.
2. Wybierz urządzenie wirtualne, które chcesz skonfigurować, a następnie kliknij ikonę **Konsola**.
3. W polu **eth0** skonfiguruj karty sieciowe urządzenia.
   Upewnij się, że automatycznie przypisane adresy DHCP (jeśli jakieś zostały przypisane) są prawidłowe w sieciach, z których korzysta maszyna wirtualna, lub przypisz je ręcznie. W zależności od liczby sieci, z których korzysta urządzenie, do skonfigurowania może być jedna lub więcej kart.
4. W polu **Scale Computing** kliknij **Zmień**, aby podać adres klastra Scale Computing HC3 i poświadczenia dostępu do niego.
   a. W polu **Nazwa / adres IP serwera** wprowadź nazwę DNS lub adres IP klastra.
   b. W polach **Nazwa użytkownika** i **Hasło** wprowadź poświadczenia dostępu do konta administratora Scale Computing HC3.
      Upewnij się, że to konto ma role wymagane do wykonywania operacji dotyczących maszyn wirtualnych Scale Computing HC3. Dodatkowe informacje na temat ról można znaleźć w sekcji "Agent dla Scale Computing HC3 (urządzenie wirtualne) — wymagane role" (s. 154).
   c. Kliknij **Sprawdź połączenie**, aby sprawdzić poprawność ustawień.
   d. Kliknij **OK**.
5. Zarejestruj urządzenie w usłudze Cyber Protection przy użyciu jednej z następujących metod.
   - [Tylko w przypadku dzierżawców, którzy nie stosują uwierzytelniania dwuskładnikowego] Zarejestruj urządzenie wirtualne w jego interfejsie graficznym.
     a. W obszarze **Opcje agenta**, w polu **Serwer zarządzania** kliknij **Zmień**.
     b. W polu **Nazwa / adres IP serwera** wybierz **Chmura**.
        Pojawi się adres usługi Cyber Protection. Nie zmieniaj tego adresu, chyba że otrzymasz inne instrukcje.

© Acronis International GmbH, 2003-2024

c. W polach **Nazwa użytkownika** i **Hasło** podaj poświadczenia dostępu do konta w usłudze Cyber Protection. Na tym koncie są rejestrowane urządzenie wirtualne i maszyny wirtualne, którymi ono zarządza.

d. Kliknij **OK**.

- Zarejestruj urządzenie w interfejsie wiersza polecenia.

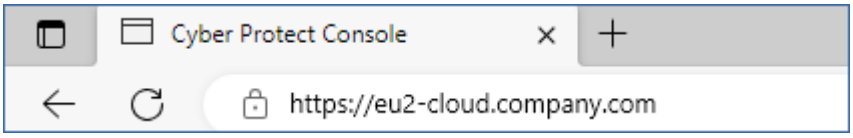
  Uwaga
  W przypadku korzystania z tej metody potrzebny jest token rejestracji. Więcej informacji o procedurze generowania tokenu można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129).

  a. Naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.

  b. Uruchom następujące polecenie:

  ```
  register_agent -o register -t cloud -a <service address> --token <registration token>
  ```

  Uwaga
  W przypadku używania tokenu rejestracji trzeba podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do konsoli Cyber Protect. Na przykład `https://eu2-cloud.company.com`.

  W tym przypadku nie używaj `https://cloud.company.com`.

  c. Aby wrócić do interfejsu graficznego urządzenia, naciśnij klawisze ALT+F1.

6. [Opcjonalnie] W polu **Nazwa** kliknij **Zmień**, aby edytować domyślną nazwę urządzenia wirtualnego (**localhost**). Nazwa ta jest wyświetlana w konsoli Cyber Protect.
7. [Opcjonalnie] W polu **Godzina** kliknij **Zmień** i wybierz strefę czasową swojej lokalizacji, aby zaplanowane operacje na pewno zostały uruchomione w odpowiednim czasie.
8. [Jeśli w sieci jest włączony serwer proxy] Skonfiguruj serwer proxy.
   a. Naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.

   b. Otwórz plik **/etc/Acronis/Global.config** w edytorze tekstowym.

   c. Wykonaj jedną z następujących czynności:
   - Jeśli ustawienia serwera proxy zostały określone podczas instalacji agenta, znajdź następującą sekcję:

   ```
   <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"1"</value>
       <value name="Host" type="TString">"ADDRESS"</value>
       <value name="Port" type="Tdword">"PORT"</value>
       <value name="Login" type="TString">"LOGIN"</value>
   ```


© Acronis International GmbH, 2003-2024

```
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- W przeciwnym wypadku skopiuj powyższe wiersze i wklej je do pliku między znacznikami `<registry name="Global">...</registry>`.

d. Zastąp wartość `ADDRESS` nową nazwą hosta / adresem IP serwera proxy, a wartość `PORT` — wartością dziesiętną numeru portu.

e. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `LOGIN` i `PASSWORD` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.

f. Zapisz plik.

g. Otwórz plik **/opt/acronis/etc/aakore.yaml** w edytorze tekstów.

h. Znajdź sekcję **env** lub ją utwórz i dodaj następujące wiersze:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Zastąp zmienne `proxy_login` i `proxy_password` poświadczeniami dostępu do serwera proxy, a zmienną `proxy_address:port` — adresem i numerem portu serwera proxy.

j. Uruchom polecenie `reboot`.

Uwaga

Aby móc zaktualizować urządzenie wirtualne wdrożone za serwerem proxy, edytuj plik `config.yaml` urządzenia (`/opt/acronis/etc/va-updater/config.yaml`), dodając następujący wiersz u dołu tego pliku, a następnie wprowadzając wartości specyficzne dla danego środowiska:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Na przykład:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Aby chronić maszyny wirtualne w klastrze Scale Computing HC3

1. Zaloguj się na koncie Cyber Protection.
2. Przejdź do sekcji **Urządzenia** > **Scale Computing HC3** > <klaster> lub znajdź komputery w sekcji **Urządzenia** > **Wszystkie urządzenia**.
3. Wybierz maszyny i zastosuj do nich plan ochrony.

Agent dla Scale Computing HC3 (urządzenie wirtualne) — wymagane role

W tej sekcji opisano role wymagane do wykonywania operacji dotyczących maszyn wirtualnych Scale Computing HC3.

© Acronis International GmbH, 2003-2024

Operacja	Rola
Tworzenie kopii zapasowych maszyn wirtualnych	Kopia zapasowa Tworzenie/edycja maszyn wirtualnych Usuwanie maszyn wirtualnych
Odzyskiwanie na istniejącą maszynę wirtualną	Kopia zapasowa Tworzenie/edycja maszyn wirtualnych Kontrola włączenia maszyn wirtualnych Usuwanie maszyn wirtualnych Ustawienia klastra
Odzyskiwanie danych na nową maszynę wirtualną	Kopia zapasowa Tworzenie/edycja maszyn wirtualnych Kontrola włączenia maszyn wirtualnych Usuwanie maszyn wirtualnych Ustawienia klastra

Wdrażanie agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne)

Zanim zaczniesz

Urządzenie to jest prekonfigurowaną maszyną wirtualną, którą użytkownik wdraża w środowisku Virtuozzo Hybrid Infrastructure. Zawiera ono agenta ochrony, który pozwala na administrowanie cyberochroną wszystkich maszyn wirtualnych w klastrze Virtuozzo Hybrid Infrastructure.

Uwaga
Aby kopie zapasowe z włączoną opcją **Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych** były odpowiednio tworzone przy użyciu danych w stanie spójności z aplikacjami, upewnij się, że na chronionych maszynach wirtualnych są zainstalowane narzędzia Virtuozzo Guest Tools w najnowszej wersji.

Wymagania systemowe agenta

Podczas wdrażania urządzenia wirtualnego można wybrać między różnymi predefiniowanymi kombinacjami procesorów vCPU i pamięci RAM (czyli wariantami). Można też utworzyć własne warianty.

W przypadku większości operacji optymalną i wystarczającą kombinacją są 2 procesory vCPU oraz 4 GB pamięci RAM. Aby poprawić wydajność tworzenia kopii zapasowych i uniknąć błędów związanych ze zbyt małą ilością pamięci RAM, w bardziej wymagających przypadkach zalecamy

© Acronis International GmbH, 2003-2024

zwiększenie tych zasobów do 4 procesorów wirtualnych i 8 GB pamięci RAM. Na przykład zwiększ przypisane zasoby, jeśli się spodziewasz, że ruch związany z tworzeniem kopii zapasowych przekroczy 100 MB na sekundę (na przykład w sieciach 10-gigabitowych), lub gdy tworzysz kopię zapasową kilku maszyn wirtualnych z dużymi dyskami twardymi (500 GB lub więcej) naraz.

Ile agentów potrzebuję?

Jeden agent może chronić cały klaster. Jeśli jednak trzeba rozłożyć obciążenie sieci ruchem związanym z tworzeniem kopii zapasowych, można mieć więcej niż jednego agenta w klastrze.

W przypadku dostępności więcej niż jednego agenta w klastrze maszyny wirtualne są automatycznie przydzielane agentom, tak aby każdy z nich zarządzał podobną liczbą maszyn.

Za każdym razem, gdy różnica obciążenia między agentami przekracza 20 procent, następuje ponowny automatyczny przydział. Może się tak zdarzyć po dodaniu bądź usunięciu jednego z komputerów lub agentów. Przykład: zauważasz potrzebę podłączenia większej liczby agentów w celu zwiększenia przepustowości i wdrażasz w klastrze dodatkowe urządzenie wirtualne. Serwer zarządzania przypisze najbardziej odpowiednie maszyny nowemu agentowi. Zmniejszy się obciążenie starszych agentów. W przypadku usunięcia agenta z serwera zarządzania komputery przydzielone do tego agenta zostaną ponownie przydzielone pozostałym agentom. Nie jest to jednak możliwe w przypadku uszkodzenia agenta lub jego ręcznego usunięcia z węzła Virtuozzo Hybrid Infrastructure. Proces ponownego przydzielania rozpocznie się dopiero po usunięciu takiego agenta z interfejsu internetowego usługi Cyber Protection.

Aby sprawdzić, który agent zarządza danym komputerem

1. W konsoli Cyber Protect kliknij **Urządzenia**, a następnie wybierz **Virtuozzo Hybrid Infrastructure**.
2. Kliknij ikonę koła zębatego w prawym górnym rogu tabeli i w obszarze **System** zaznacz pole wyboru **Agent**.
3. Sprawdź nazwę agenta w wyświetlonej kolumnie.

Ograniczenia

- Urządzenia Virtuozzo Hybrid Infrastructure nie można wdrożyć zdalnie.
- Tworzenie kopii zapasowych maszyn wirtualnych uwzględniających aplikacje nie jest obsługiwane.

Konfigurowanie sieci w środowisku Virtuozzo Hybrid Infrastructure

Przed wdrożeniem i skonfigurowaniem urządzenia wirtualnego trzeba skonfigurować sieci w środowisku Virtuozzo Hybrid Infrastructure.

Sieciowe wymagania agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne)

- Urządzenie wirtualne wymaga 2 kart sieciowych.
- Urządzenie wirtualne musi być podłączone do sieci Virtuozzo obsługującej następujące typy ruchu sieciowego:

© Acronis International GmbH, 2003-2024

- Compute API (Obliczenia interfejsu API)
- VM Backups (Kopie zapasowe maszyn wirtualnych)
- ABGW Public (Publiczny ruch ABGW)
- VM Public (Publiczny ruch maszyn wirtualnych)

Dodatkowe informacje na temat konfigurowania sieci można znaleźć w sekcji Compute cluster requirements (Wymagania klastra obliczeniowego) w dokumentacji rozwiązania Virtuozzo.

Konfigurowanie kont użytkowników w środowisku Virtuozzo Hybrid Infrastructure

Aby skonfigurować urządzenie wirtualne, potrzebujesz konta użytkownika w środowisku Virtuozzo Hybrid Infrastructure. Konto musi mieć rolę **Administrator** w domenie **Default** (Domyślna). Dodatkowe informacje na temat użytkowników można znaleźć w sekcji Managing admin panel users (Zarządzanie użytkownikami panelu administracyjnego) w dokumentacji środowiska Virtuozzo Hybrid Infrastructure. Upewnij się, że konto ma przyznany dostęp do wszystkich projektów w domenie **Default** (Domyślna).

Aby przyznać dostęp do wszystkich projektów w domenie Default (Domyślna)

1. Utwórz plik środowiskowy dla administratora systemu. W tym celu uruchom następujący skrypt w klastrze Virtuozzo Hybrid Infrastructure za pomocą interfejsu wiersza polecenia narzędzia OpenStack. Więcej informacji na temat możliwości nawiązania połączenia z tym interfejsem można znaleźć w sekcji Connecting to OpenStack Command-Line Interface (Nawiązywanie połączenia z interfejsem wiersza polecenia) w dokumentacji środowiska Virtuozzo Hybrid Infrastructure.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. Za pomocą pliku środowiskowego autoryzuj kolejne polecenia narzędzia OpenStack:

   ```
   . /etc/kolla/admin-openrc.sh
   ```

3. Uruchom następujące polecenia:

   ```
   openstack --insecure user set --project admin --project-domain Default --domain
   Default <username>
   openstack --insecure role add --domain Default --user <username> --user-domain
   Default compute --inherited
   ```

   Tutaj <username> (nazwa użytkownika) oznacza konto w środowisku Virtuozzo Hybrid Infrastructure z rolą **Administrator** w domenie **Default** (Domyślna). Urządzenie wirtualne będzie używało tego konta do tworzenia kopii zapasowych i przywracania maszyn wirtualnych w dowolnym projekcie podrzędnym w ramach domeny **Default** (Domyślna).

© Acronis International GmbH, 2003-2024

Przykład

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

Aby zarządzać kopiami zapasowymi maszyn wirtualnych w domenie innej niż **Default** (Domyślna), uruchom również poniższe polecenie.

Aby przyznać dostęp do wszystkich projektów w innej domenie

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

Tutaj <domain name> (nazwa domeny) oznacza domenę zawierającą projekty, do których będzie miało dostęp konto <username> (nazwa użytkownika).

Przykład

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

Po przyznaniu dostępu do projektów sprawdź, jakie role są przypisane do konta.

Aby sprawdzić przypisane role

```
openstack --insecure role assignment list --user <username> --names
```

Tutaj <username> (nazwa użytkownika) oznacza konto w środowisku Virtuozzo Hybrid Infrastructure.

Przykład

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```


© Acronis International GmbH, 2003-2024

W tym przykładzie opcje `-c Role`, `-c User`, `-c Project` i `-c Domain` mają na celu skrócenie wyników wykonywania poleceń, tak aby zmieściły się na stronie.

Aby sprawdzić, jakie efektywne role są przypisane do konta we wszystkich projektach, uruchom również następujące polecenie.

Aby sprawdzić efektywne role we wszystkich projektach

```
openstack --insecure role assignment list --user <username> --names --effective
```

Tutaj <username> (nazwa użytkownika) oznacza konto w środowisku Virtuozzo Hybrid Infrastructure.

Przykład

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

W tym przykładzie opcje `-c Role`, `-c User`, `-c Project` i `-c Domain` mają na celu skrócenie wyników wykonywania poleceń, tak aby zmieściły się na stronie.

Wdrażanie szablonu QCOW2

1. Zaloguj się na koncie Cyber Protection.
2. Kliknij **Urządzenia** > **Wszystkie urządzenia** > **Dodaj** > **Virtuozzo Hybrid Infrastructure**.
   Na Twoją maszynę zostanie pobrane archiwum zip.
3. Rozpakuj archiwum .zip. Zawiera on plik obrazu .qcow2.
4. Zaloguj się na koncie w środowisku Virtuozzo Hybrid Infrastructure.
5. Dodaj plik obrazu .qcow2 do klastra obliczeniowego Virtuozzo Hybrid Infrastructure. W tym celu:

© Acronis International GmbH, 2003-2024

- Na karcie **Obliczenia** > **Maszyny wirtualne** > **Obrazy** kliknij **Dodaj obraz**.
- W oknie **Dodaj obraz** kliknij **Przeglądaj**, a następnie zaznacz plik .qcow2.
- Podaj nazwę obrazu, wybierz typ **Nieokreślony system operacyjny Linux** i kliknij **Dodaj**.

6. Na karcie **Obliczenia** > **Maszyny wirtualne** > **Maszyny wirtualne** kliknij **Utwórz maszynę wirtualną**. Zostanie otwarte okno, w którym należy określić następujące parametry:
   - Nazwa nowej maszyny wirtualnej.
   - W sekcji **Wdróż z** wybierz **Obraz**.
   - W oknie **Obrazy** wybierz plik obrazu .qcow2 urządzenia, a następnie kliknij **Gotowe**.
   - W oknie **Woluminy** nie trzeba dodawać żadnych woluminów. Wolumin dodany automatycznie do dysku systemowego wystarcza.
   - W oknie **Wariant** wybierz żądaną kombinację procesorów vCPU i pamięci RAM, a następnie kliknij **Gotowe**. Zwykle wystarczą 2 procesory vCPU i 4 GB pamięci RAM.
   - W oknie **Interfejsy sieciowe** kliknij **Dodaj**, wybierz *publiczną* sieć wirtualną, a następnie kliknij **Dodaj**. Pozycja ta pojawi się na liście **Interfejsy sieciowe**.
     Jeśli używasz konfiguracji z więcej niż jedną siecią fizyczną (a więc i więcej niż jedną publiczną siecią wirtualną), powtórz ten krok i wybierz potrzebne sieci wirtualne.
7. Kliknij **Gotowe**.
8. Po powrocie do okna **Utwórz maszynę wirtualną** kliknij **Wdróż**, aby utworzyć i uruchomić maszynę wirtualną.

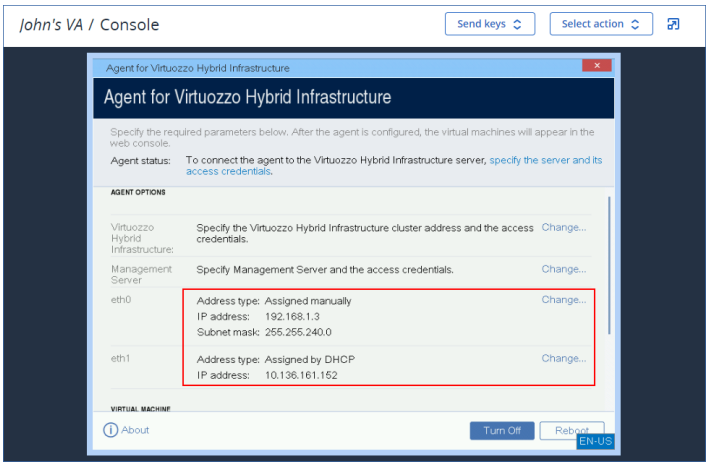
Konfigurowanie urządzenia wirtualnego

Po wdrożeniu agenta dla Virtuozzo Hybrid Infrastructure (urządzenia wirtualnego) należy skonfigurować to urządzenie wirtualne tak, aby miało dostęp zarówno do klastra Virtuozzo Hybrid Infrastructure, które będzie chronić, jak i do usługi chmury Cyber Protection.

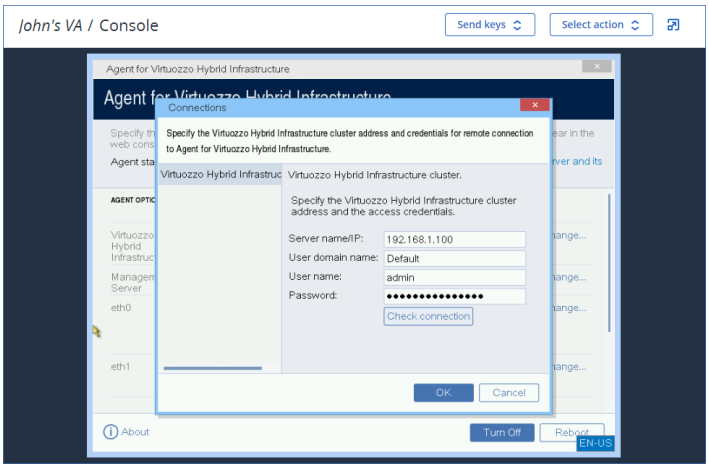
Aby skonfigurować urządzenie wirtualne

1. Zaloguj się na koncie w środowisku Virtuozzo Hybrid Infrastructure.
2. Na karcie **Obliczenia** > **Maszyny wirtualne** > **Maszyny wirtualne** zaznacz utworzoną maszynę wirtualną. Następnie kliknij **Konsola**.
3. Skonfiguruj interfejsy sieciowe urządzenia. Może być jeden lub kilka interfejsów do skonfigurowania — to zależy to od liczby sieci wirtualnych, z których korzysta urządzenie. Upewnij się, że automatycznie przypisane adresy DHCP (jeśli jakieś zostały przypisane) są prawidłowe w sieciach, z których korzysta maszyna wirtualna, lub przypisz je ręcznie.

© Acronis International GmbH, 2003-2024



4. Podaj adres klastra Virtuozzo i poświadczenia:
   - Nazwa DNS lub adres IP klastra Virtuozzo Hybrid Infrastructure — jest to adres węzła zarządzania klastra. Domyślnie zostanie automatycznie ustawiony port 5000. Jeśli chcesz użyć innego portu, trzeba go określić ręcznie.
   - W polu **Nazwa domeny użytkownika** wskaż domenę w środowisku Virtuozzo Hybrid Infrastructure. Na przykład **Default** (Domyślna).
     W nazwie domeny jest uwzględniana wielkość liter.
   - W polach **Nazwa użytkownika** i **Hasło** wprowadź poświadczenia dostępu do konta w środowisku Virtuozzo Hybrid Infrastructure z rolą **Administrator** we wskazanej domenie.
     Więcej informacji na temat użytkowników, ról i domen można znaleźć w sekcji Konfigurowanie kont użytkowników w środowisku Virtuozzo Hybrid Infrastructure.



5. Zarejestruj urządzenie w usłudze Cyber Protection przy użyciu jednej z następujących metod.
   - [Tylko w przypadku dzierżawców, którzy nie stosują uwierzytelniania dwuskładnikowego] Zarejestruj urządzenie wirtualne w jego interfejsie graficznym.
     a. W obszarze **Opcje agenta**, w polu **Serwer zarządzania** kliknij **Zmień**.
     b. W polu **Nazwa / adres IP serwera** wybierz **Chmura**.
        Pojawi się adres usługi Cyber Protection. Nie zmieniaj tego adresu, chyba że otrzymasz inne instrukcje.

© Acronis International GmbH, 2003-2024

c. W polach **Nazwa użytkownika** i **Hasło** podaj poświadczenia dostępu do konta w usłudze Cyber Protection. Na tym koncie są rejestrowane urządzenie wirtualne i maszyny wirtualne, którymi ono zarządza.

d. Kliknij **OK**.

- Zarejestruj urządzenie w interfejsie wiersza polecenia.

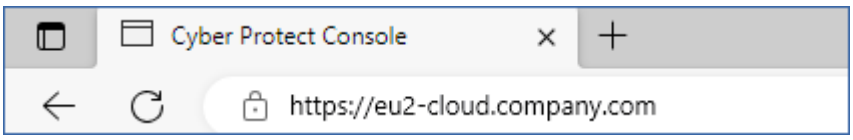
Uwaga
W przypadku korzystania z tej metody potrzebny jest token rejestracji. Więcej informacji o procedurze generowania tokenu można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129).

a. Naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.

b. Uruchom następujące polecenie:

```
register_agent -o register -t cloud -a <service address> --token <registration token>
```

Uwaga
W przypadku używania tokenu rejestracji trzeba podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do konsoli Cyber Protect. Na przykład `https://eu2-cloud.company.com`.



W tym przypadku nie używaj `https://cloud.company.com`.

c. Aby wrócić do interfejsu graficznego urządzenia, naciśnij klawisze ALT+F1.

6. [Jeśli w sieci jest włączony serwer proxy] Skonfiguruj serwer proxy.

a. Naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.

b. Otwórz plik **/etc/Acronis/Global.config** w edytorze tekstowym.

c. Wykonaj jedną z następujących czynności:

- Jeśli ustawienia serwera proxy zostały określone podczas instalacji agenta, znajdź następującą sekcję:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- W przeciwnym wypadku skopiuj powyższe wiersze i wklej je do pliku między znacznikami `<registry name="Global">...</registry>`.

© Acronis International GmbH, 2003-2024

d. Zastąp wartość `ADDRESS` nową nazwą hosta / adresem IP serwera proxy, a wartość `PORT` — wartością dziesiętną numeru portu.
e. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `LOGIN` i `PASSWORD` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.
f. Zapisz plik.
g. Otwórz plik **/opt/acronis/etc/aakore.yaml** w edytorze tekstów.
h. Znajdź sekcję **env** lub ją utwórz i dodaj następujące wiersze:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Zastąp zmienne `proxy_login` i `proxy_password` poświadczeniami dostępu do serwera proxy, a zmienną `proxy_address:port` — adresem i numerem portu serwera proxy.
j. Uruchom polecenie `reboot`.

Uwaga
Aby móc zaktualizować urządzenie wirtualne wdrożone za serwerem proxy, edytuj plik `config.yaml` urządzenia (`/opt/acronis/etc/va-updater/config.yaml`), dodając następujący wiersz u dołu tego pliku, a następnie wprowadzając wartości specyficzne dla danego środowiska:

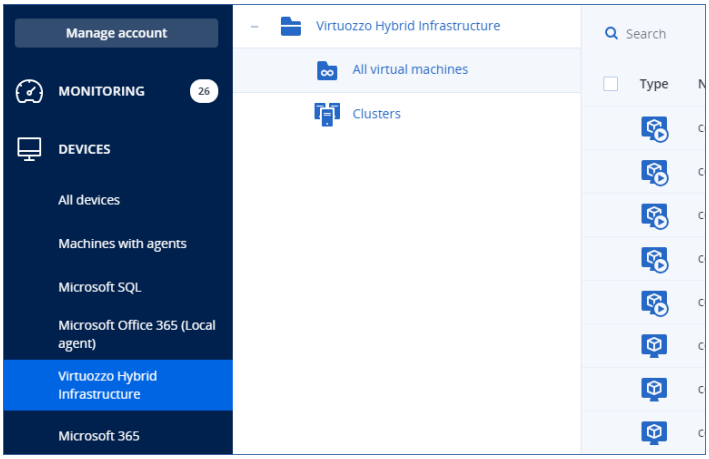
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Na przykład:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Aby chronić maszyny wirtualne w klastrze Virtuozzo Hybrid Infrastructure

1. Zaloguj się na koncie Cyber Protection.
2. Przejdź do sekcji **Urządzenia** > **Virtuozzo Hybrid Infrastructure** > <Twój klaster> > **Projekt domyślny** > **administrator** lub znajdź maszyny w sekcji **Urządzenia** > **Wszystkie urządzenia**.
3. Wybierz maszyny i zastosuj do nich plan ochrony.



© Acronis International GmbH, 2003-2024

Wdrażanie agenta dla oVirt (urządzenie wirtualne)

Zanim zaczniesz

Urządzenie to jest prekonfigurowaną maszyną wirtualną wdrażaną w centrum danych Red Hat Virtualization / oVirt. Urządzenie zawiera agenta ochrony, który pozwala na administrowanie ochroną cybernetyczną wszystkich maszyn wirtualnych w centrum danych.

Wymagania systemowe agenta

Domyślnie maszyna wirtualna z agentem używa 2 procesorów vCPU i 4 GiB pamięci RAM. Ustawienia te są wystarczające w przypadku większości operacji, ale można je edytować w portalu administracji Red Hat Virtualization / oVirt.

Aby poprawić wydajność tworzenia kopii zapasowych i uniknąć błędów związanych ze zbyt małą ilością pamięci RAM, w bardziej wymagających przypadkach zalecamy zwiększenie tych zasobów do 4 procesorów wirtualnych i 8 GiB pamięci RAM. Na przykład zwiększ przypisane zasoby, jeśli się spodziewasz, że ruch związany z tworzeniem kopii zapasowych przekroczy 100 MB na sekundę (na przykład w sieciach 10-gigabitowych), lub gdy tworzysz kopię zapasową kilku maszyn wirtualnych z dużymi dyskami twardymi (500 GB lub więcej) naraz.

Dysk wirtualny urządzenia ma rozmiar 8 GiB.

Ile agentów potrzebuję?

Jeden agent może chronić całe centrum danych. Jeśli jednak trzeba rozłożyć obciążenie sieci ruchem związanym z tworzeniem kopii zapasowych, można mieć więcej niż jednego agenta w centrum danych.

W przypadku dostępności więcej niż jednego agenta w centrum danych maszyny wirtualne są automatycznie przydzielane agentom, tak aby każdy z nich zarządzał podobną liczbą maszyn.

Za każdym razem, gdy różnica obciążenia między agentami przekracza 20 procent, następuje ponowny automatyczny przydział. Może się tak zdarzyć po dodaniu bądź usunięciu jednego z komputerów lub agentów. Przykład: zauważasz potrzebę podłączenia większej liczby agentów w celu zwiększenia przepustowości i wdrażasz w centrum danych dodatkowe urządzenie wirtualne. Serwer zarządzania przypisze najbardziej odpowiednie maszyny nowemu agentowi. Zmniejszy się obciążenie starszych agentów. W przypadku usunięcia agenta komputery przydzielone do tego agenta zostaną przydzielone pozostałym agentom. Nie jest to jednak możliwe w przypadku uszkodzenia agenta lub jego ręcznego usunięcia z portalu administracji Red Hat Virtualization / oVirt. Proces ponownego przydzielania rozpocznie się dopiero po usunięciu takiego agenta z konsoli Cyber Protect.

Aby sprawdzić, który agent zarządza danym komputerem

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect kliknij **Urządzenia**, a następnie wybierz **oVirt**.
2. Kliknij ikonę koła zębatego w prawym górnym rogu tabeli i w obszarze **System** zaznacz pole wyboru **Agent**.
3. Sprawdź nazwę agenta w wyświetlonej kolumnie.

Ograniczenia

Poniższe operacje nie są obsługiwane w przypadku maszyn wirtualnych Red Hat Virtualization / oVirt:

- Kopia zapasowa uwzględniająca aplikacje
- Uruchamianie maszyny wirtualnej z kopii zapasowej
- Replikacja maszyn wirtualnych
- Śledzenie zmienionych bloków

© Acronis International GmbH, 2003-2024

Wdrażanie szablonu OVA

1. Zaloguj się na koncie Cyber Protection.
2. Kliknij **Urządzenia** > **Wszystkie urządzenia** > **Dodaj** > **Red Hat Virtualization (oVirt)**.
   Na Twoją maszynę zostanie pobrane archiwum zip.
3. Rozpakuj archiwum .zip. Zawiera ono jeden plik .ova.
4. Prześlij plik .ova na host w centrum danych Red Hat Virtualization / oVirt, które chcesz chronić.
5. Zaloguj się do portalu administracji Red Hat Virtualization / oVirt jako administrator. Dodatkowe informacje na temat ról wymaganych do operacji dotyczących maszyn wirtualnych można znaleźć w sekcji "Agent dla oVirt — wymagane role i porty" (s. 170).
6. W menu nawigacyjnym wybierz **Compute** (Obliczenia) > **Virtual machines** (Maszyny wirtualne).
7. Kliknij ikonę pionowego wielokropka nad główną tabelą, a następnie kliknij **Import** (Importuj).
8. W oknie **Import Virtual Machine(s)** (Importuj maszyny wirtualne) zrób tak:
   a. W polu **Data center** (Centrum danych) wybierz centrum danych, które chcesz chronić.
   b. W polu **Source** (Źródło) wybierz **Virtual Appliance (OVA)** (Urządzenie wirtualne [OVA]).
   c. W polu **Host** wybierz host, na który został przesłany plik .ova.
   d. W polu **File Path** (Ścieżka do pliku) podaj ścieżkę do katalogu zawierającego plik .ova.
   e. Kliknij **Load** (Załaduj).
      Na panelu **Virtual Machines on Source** (Maszyny wirtualne w źródle) pojawi się szablon urządzenia wirtualnego oVirt z pliku .ova.
      Jeśli szablon nie pojawi się na tym panelu, upewnij się, że została podana poprawna ścieżka pliku oraz że plik nie jest uszkodzony i działa komunikacja z hostem.
   f. Na panelu **Virtual Machines on Source** (Maszyny wirtualne w źródle) wybierz szablon urządzenia wirtualnego oVirt, a następnie kliknij strzałkę w prawo.
      Szablon pojawi się na panelu **Virtual machines to import** (Maszyny wirtualne do zaimportowania).
   g. Kliknij **Dalej**.
9. W nowym oknie kliknij nazwę urządzenia, a następnie skonfiguruj następujące ustawienia:
   - Na karcie **Network interfaces** (Karty sieciowe) skonfiguruj karty sieciowe.
   - [Opcjonalnie] Na karcie **General** (Ogólne) zmień domyślną nazwę maszyny wirtualnej z zainstalowanym agentem.

Wdrożenie zostało ukończone. Teraz trzeba skonfigurować urządzenie wirtualne. Dodatkowe informacje na temat jego konfigurowania można znaleźć w sekcji "Konfigurowanie urządzenia wirtualnego" (s. 167).

© Acronis International GmbH, 2003-2024

Uwaga
Jeśli w centrum danych jest potrzebne więcej niż jedno urządzenie wirtualne, powtórz powyższe kroki i wdróż dodatkowe urządzenia. Nie klonuj istniejącego już urządzenia wirtualnego przy użyciu opcji **Clone VM** (Klonuj maszynę wirtualną) w portalu administracji Red Hat Virtualization / oVirt.

Aby wykluczyć urządzenie wirtualne z kopii zapasowych grupy dynamicznej, trzeba je wykluczyć również z listy maszyn wirtualnych w konsoli Cyber Protect. W tym celu w portalu administracji Red Hat Virtualization / oVirt wybierz maszynę wirtualną z agentem, a następnie przypisz jej znacznik `acronis_virtual_appliance`.

Konfigurowanie urządzenia wirtualnego

Po wdrożeniu urządzenia wirtualnego należy je skonfigurować tak, aby miało dostęp zarówno do mechanizmu oVirt, jak i do usługi Cyber Protection.

Aby skonfigurować urządzenie wirtualne

1. Zaloguj się do portalu administracji Red Hat Virtualization / oVirt.
2. Wybierz urządzenie wirtualne, które chcesz skonfigurować, a następnie kliknij ikonę **Konsola**.
3. W polu **eth0** skonfiguruj karty sieciowe urządzenia.
   Upewnij się, że automatycznie przypisane adresy DHCP (jeśli jakieś zostały przypisane) są prawidłowe w sieciach, z których korzysta maszyna wirtualna, lub przypisz je ręcznie. W zależności od liczby sieci, z których korzysta urządzenie, do skonfigurowania może być jedna lub więcej kart.
4. W polu **oVirt** kliknij **Zmień**, aby podać adres mechanizmu oVirt i poświadczenia dostępu do niego:
   a. W polu **Nazwa / adres IP serwera** wprowadź nazwę DNS lub adres IP mechanizmu.
   b. W polach **Nazwa użytkownika** i **Hasło** wprowadź poświadczenia administratora dotyczące mechanizmu.
      Upewnij się, że to konto administratora ma role wymagane do pracy z maszynami wirtualnymi Red Hat Virtualization / oVirt. Dodatkowe informacje na temat ról można znaleźć w sekcji "Agent dla oVirt — wymagane role i porty" (s. 170).
      Jeśli dostawcą usług pojedynczego logowania (Single-Sign-On, SSO) dla mechanizmu oVirt jest Keycloak (domyślnie w oVirt w wersji 4.5.1), podczas podawania nazwy użytkownika użyj formatu rozwiązania Keycloak. Na przykład wpisz domyślne konto administratora jako `admin@ovirt@internalsso`, a nie `admin@internal`.
   c. [Opcjonalnie] Kliknij **Sprawdź połączenie**, aby sprawdzić, czy podane poświadczenia są poprawne.
   d. Kliknij **OK**.
5. Zarejestruj urządzenie w usłudze Cyber Protection przy użyciu jednej z następujących metod.
   - [Tylko w przypadku dzierżawców, którzy nie stosują uwierzytelniania dwuskładnikowego] Zarejestruj urządzenie wirtualne w jego interfejsie graficznym.

© Acronis International GmbH, 2003-2024

a. W obszarze **Opcje agenta**, w polu **Serwer zarządzania** kliknij **Zmień**.

b. W polu **Nazwa / adres IP serwera** wybierz **Chmura**.

   Pojawi się adres usługi Cyber Protection. Nie zmieniaj tego adresu, chyba że otrzymasz inne instrukcje.

c. W polach **Nazwa użytkownika** i **Hasło** podaj poświadczenia dostępu do konta w usłudze Cyber Protection. Na tym koncie są rejestrowane urządzenie wirtualne i maszyny wirtualne, którymi ono zarządza.

d. Kliknij **OK**.

- Zarejestruj urządzenie w interfejsie wiersza polecenia.

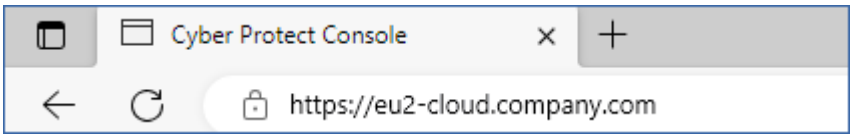
  Uwaga
  W przypadku korzystania z tej metody potrzebny jest token rejestracji. Więcej informacji o procedurze generowania tokenu można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129).

  a. Naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.

  b. Uruchom następujące polecenie:

  ```
  register_agent -o register -t cloud -a <service address> --token <registration token>
  ```

  Uwaga
  W przypadku używania tokenu rejestracji trzeba podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do konsoli Cyber Protect. Na przykład `https://eu2-cloud.company.com`.

  W tym przypadku nie używaj `https://cloud.company.com`.

  c. Aby wrócić do interfejsu graficznego urządzenia, naciśnij klawisze ALT+F1.

6. [Opcjonalnie] W polu **Nazwa** kliknij **Zmień**, aby edytować domyślną nazwę urządzenia wirtualnego (**localhost**). Nazwa ta jest wyświetlana w konsoli Cyber Protect.
7. [Opcjonalnie] W polu **Godzina** kliknij **Zmień** i wybierz strefę czasową swojej lokalizacji, aby zaplanowane operacje na pewno zostały uruchomione w odpowiednim czasie.
8. [Opcjonalnie] [Jeśli w sieci jest włączony serwer proxy] Skonfiguruj serwer proxy.
   a. Naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.
   b. Otwórz plik **/etc/Acronis/Global.config** w edytorze tekstowym.
   c. Wykonaj jedną z następujących czynności:
      - Jeśli ustawienia serwera proxy zostały określone podczas instalacji agenta, znajdź następującą sekcję:

© Acronis International GmbH, 2003-2024

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- W przeciwnym wypadku skopiuj powyższe wiersze i wklej je do pliku między znacznikami `<registry name="Global">...</registry>`.

d. Zastąp wartość `ADDRESS` nową nazwą hosta / adresem IP serwera proxy, a wartość `PORT` — wartością dziesiętną numeru portu.

e. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `LOGIN` i `PASSWORD` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.

f. Zapisz plik.

g. Otwórz plik **/opt/acronis/etc/aakore.yaml** w edytorze tekstów.

h. Znajdź sekcję **env** lub ją utwórz i dodaj następujące wiersze:

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Zastąp zmienne `proxy_login` i `proxy_password` poświadczeniami dostępu do serwera proxy, a zmienną `proxy_address:port` — adresem i numerem portu serwera proxy.

j. Uruchom polecenie `reboot`.

Uwaga

Aby móc zaktualizować urządzenie wirtualne wdrożone za serwerem proxy, edytuj plik `config.yaml` urządzenia (`/opt/acronis/etc/va-updater/config.yaml`), dodając następujący wiersz u dołu tego pliku, a następnie wprowadzając wartości specyficzne dla danego środowiska:

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

Na przykład:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Aby chronić maszyny wirtualne w centrum danych Red Hat Virtualization / oVirt

1. Zaloguj się na koncie Cyber Protection.
2. Przejdź do sekcji **Urządzenia** > **oVirt** > <klaster> lub znajdź komputery w sekcji **Urządzenia** > **Wszystkie urządzenia**.
3. Wybierz maszyny i zastosuj do nich plan ochrony.

© Acronis International GmbH, 2003-2024

Agent dla oVirt — wymagane role i porty

Wymagane role

Do wdrożenie i działania agenta dla oVirt wymagane jest konta administratora z przypisanymi następującymi rolami.

oVirt / Red Hat Virtualization 4.2 i 4.3 / Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt / Red Hat Virtualization 4.4, 4.5

- SuperUser

Wymagane porty

Agent dla oVirt łączy się z mechanizmem oVirt przy użyciu adresu URL podanego podczas konfiguracji urządzenia wirtualnego. Zazwyczaj adres URL tego mechanizmu ma następujący format: `https://ovirt.nazwa_firmy.com`. W tym przypadku używany jest protokół HTTPS i port 443.

Ustawienia oVirt inne niż domyślne mogą wymagać innego portu. Dokładny port można ustalić dzięki analizie formatu adresu URL. Na przykład:

Adres URL mechanizmu oVirt	Port	Protokół
`https://ovirt.nazwa_firmy.com/`	443	HTTPS
`http://ovirt.nazwa_firmy.com/`	80	HTTP
`https://ovirt.nazwa_firmy.com:1234/`	1234	HTTPS

Do operacji odczytu/zapisu dysku nie są wymagane żadne dodatkowe porty, ponieważ kopia zapasowa jest tworzona w trybie HotAdd.

Wdrażanie agenta dla Synology

Zanim zaczniesz

Za pomocą agenta dla Synology można tworzyć kopie zapasowe plików i folderów z urządzeń oraz na urządzenia Synology NAS. Właściwości i uprawnienia dostępu dotyczące udziałów, folderów i plików na urządzeniach NAS zostaną zachowane.

© Acronis International GmbH, 2003-2024

Agent dla Synology działa na urządzeniu NAS. Dzięki temu można wykorzystać zasoby urządzenia do wykonywania operacji przetwarzania danych poza hostem, takich jak replikacja, sprawdzanie poprawności i czyszczenie kopii zapasowych. Dodatkowe informacje na temat tych operacji można znaleźć w sekcji "Plany ochrony danych poza hostem" (s. 230).

Uwaga
Agent dla Synology obsługuje tylko urządzenia NAS z procesorami x86_64. Procesory ARM nie są obsługiwane.

Kopię zapasową można odzyskać do pierwotnej lub nowej lokalizacji na urządzeniu NAS oraz do folderu sieciowego, który jest dostępny za pośrednictwem tego urządzenia. Kopie zapasowe przechowywane w chmurze można też odzyskać na inne niż pierwotne urządzenie NAS, na którym jest zainstalowany agent dla Synology.

Poniższa tabela zawiera zestawienie dostępnych źródeł i miejsc docelowych kopii zapasowych.

Elementy uwzględniane w kopii zapasowej	**Elementy uwzględniane w kopii zapasowej (Źródło kopii zapasowej)**	**Miejsce docelowe kopii zapasowej (Miejsce docelowe kopii zapasowej)**
Pliki/foldery	Folder lokalny*	Chmura
		Folder lokalny*
	Folder sieciowy (SMB)**	Folder sieciowy (SMB)**
		Folder NFS
		Chmury publiczne***

* W tym dyski USB podłączone do urządzenia NAS.

Uwaga
Foldery zaszyfrowane nie są obsługiwane. Te foldery nie są wyświetlane w graficznym interfejsie użytkownika oprogramowania Cyber Protection.

** Możliwość używania zewnętrznych udziałów sieciowych jako źródeł lub miejsc docelowych kopii zapasowych za pośrednictwem protokołu SMB jest dostępna tylko w przypadku agentów działających w systemie Synology DiskStation Manager w wersji 6.2.3 lub nowszej. Kopie zapasowe danych przechowywanych na samym serwerze Synology NAS, w tym hostowanych udziałach sieciowych, można tworzyć bez ograniczeń.

*** Tworzenie kopii zapasowych w chmurach publicznych, takich jak Microsoft Azure, Amazon, Wasabi lub magazyny zgodne z S3, jest obsługiwane tylko przez agenta dla Synology 7.x. Agent dla Synology 6.x nie obsługuje tego miejsca docelowego kopii zapasowych ze względu na ograniczenia jądra systemu Linux rozwiązania Synology DSM 6.x.

© Acronis International GmbH, 2003-2024

Ograniczenia

- Agent dla Synology obsługuje tylko urządzenia NAS z procesorami x86_64. Procesory ARM nie są obsługiwane.
- Zaszyfrowane udziały z kopii zapasowej są odzyskiwane jako niezaszyfrowane.
- Udziały, w których przypadku włączono opcję **Kompresja plików**, są odzyskiwane z kopii zapasowej jako udziały z wyłączoną tą opcją.
- Na urządzenie Synology NAS można odzyskiwać tylko kopie zapasowe utworzone przez agenta dla Synology.

Pobieranie programu instalacyjnego

Program instalacyjny agenta dla Synology jest dostępny w formie pliku SPK.

Agent dla Synology 7.x

Aby pobrać program instalacyjny

1. W konsoli usługi Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. W prawym górnym rogu kliknij **Dodaj**.
3. W obszarze **Sieciowa pamięć masowa (NAS)** kliknij **Synology**.
   Program instalacyjny zostanie pobrany na Twój komputer.

Agent dla Synology 6.x

Aby pobrać program instalacyjny

1. W konsoli usługi Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. W prawym górnym rogu kliknij **Dodaj**.
3. W obszarze **Sieciowa pamięć masowa (NAS)** kliknij **Synology**.
   Rozpocznie się pobieranie programu instalacyjnego agenta dla Synology 7.x na komputer.
   Możesz bezpiecznie zatrzymać proces pobierania lub zignorować pobrany plik.
4. Kliknij **Pobierz agenta dla Synology 6.x**.
   Rozpocznie się pobieranie programu instalacyjnego agenta dla Synology 6.x na komputer.

Instalowanie agenta dla Synology

Aby zainstalować agenta dla Synology, uruchom plik SPK w systemie Synology DiskStation Manager.

Uwaga
Agent dla Synology obsługuje tylko urządzenia NAS z procesorami x86_64. Procesory ARM nie są obsługiwane.

Agent dla Synology 7.x

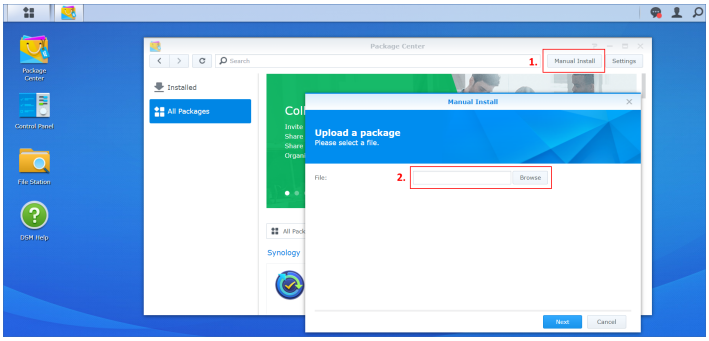
© Acronis International GmbH, 2003-2024

Wymagania wstępne

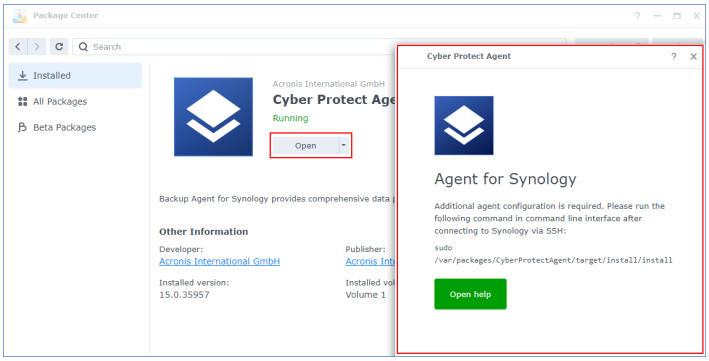
- Na urządzeniu NAS działa system DiskStation Manager 7.x.
- Należysz do grupy **administratorów** na urządzeniu NAS.
- Na woluminie NAS, na którym chcesz zainstalować agenta, jest co najmniej 200 MB wolnego miejsca.
- Na komputerze jest dostępny klient SSH. W tym dokumencie na potrzeby przykładu użyto narzędzia Putty.

Aby zainstalować agenta dla Synology

1. Zaloguj się do systemu Synology DiskStation Manager.
2. Otwórz okno **Package Center** (Centrum pakietów).
3. Kliknij **Manual Install** (Instalacja ręczna), a następnie kliknij **Browse** (Przeglądaj).



4. Wybierz plik SPK pobrany z konsoli Cyber Protect, a następnie kliknij **Next** (Dalej).
   Zostanie wyświetlone ostrzeżenie, że jest instalowany pakiet oprogramowania innej firmy. Komunikat ten stanowi część standardowej procedury instalacji.
5. Aby potwierdzić, że chcesz zainstalować pakiet, kliknij **Agree** (Zgadzam się).
6. Wybierz wolumin, na którym chcesz zainstalować agenta, a następnie kliknij **Next** (Dalej).
7. Sprawdź ustawienia i kliknij **Done** (Gotowe).
8. W sekcji **Package Center** (Centrum pakietów) systemu Synology DiskStation Manager otwórz narzędzie Cyber Protect Agent for Synology, a następnie sprawdź, czy jest widoczny następujący ekran.



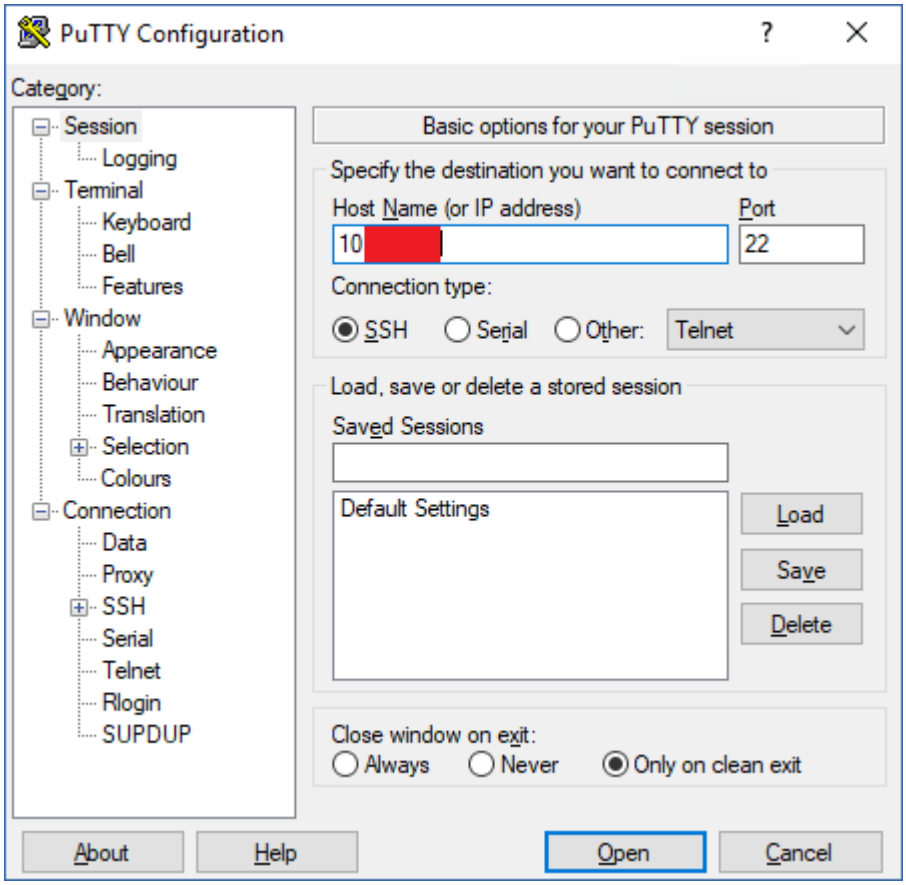
9. W sekcji **Control Panel** (Panel sterowania) systemu Synology DiskStation Manager przejdź do sekcji **Terminal & SNMP** (Terminal i protokół SNMP) i włącz dostęp SSH do urządzenia NAS.

© Acronis International GmbH, 2003-2024

10. Uruchom skrypt `install` na urządzeniu NAS przy użyciu klienta SSH (w tym przykładzie: narzędzia Putty).

    Skrypt ten umożliwia dostęp na poziomie użytkownika root do systemu DSM 7.0 lub nowszego, który jest wymagany do skonfigurowania agenta.

    a. Uruchom narzędzie Putty, a następnie podaj adres IP lub nazwę hosta urządzenia Synology NAS.



    b. Kliknij **Open** (Otwórz) i się zaloguj jako administrator systemu Synology DSM.

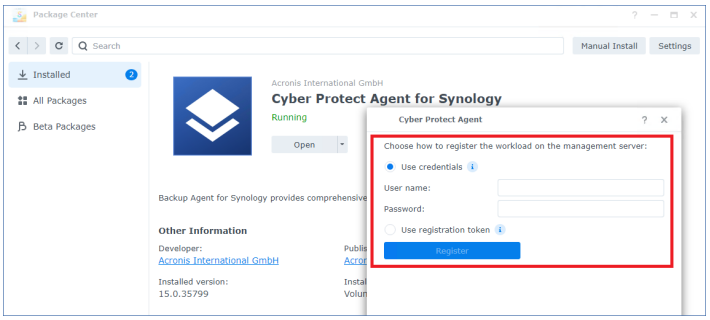
    c. Uruchom następujące polecenie.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

    Po uruchomieniu skryptu odczekaj 15 sekund, podczas których są inicjowane usługi Cyber Protection.

11. W sekcji **Control Panel** (Panel sterowania) systemu Synology DiskStation Manager przejdź do sekcji **Terminal & SNMP** (Terminal i protokół SNMP) i wyłącz dostęp SSH do urządzenia NAS. Dostęp SSH nie jest już wymagany.
12. W sekcji **Package Center** (Centrum pakietów) systemu Synology DiskStation Manager otwórz narzędzie Cyber Protect Agent for Synology.
13. Wybierz metodę rejestracji.

© Acronis International GmbH, 2003-2024



- [Aby zarejestrować agenta przy użyciu poświadczeń]
  - W polach **Nazwa użytkownika** i **Hasło** podaj poświadczenia dostępu do konta, na którym będzie zarejestrowany agent. Konto to nie może być kontem administratora partnera.
- [Aby zarejestrować agenta przy użyciu tokenu rejestracji]
  - W polu **Adres rejestracji** podaj dokładny adres centrum danych. Dokładny adres centrum danych to adres URL widoczny po zalogowaniu się w konsoli Cyber Protect. Na przykład `https://us5-cloud.acronis.com`.

    Uwaga
    Nie używaj formatu URL bez adresu centrum danych. Na przykład nie używaj adresu `https://cloud.acronis.com`.

  - W polu **Token** podaj token rejestracji.

    Dodatkowe instrukcje dotyczące generowania tokenu rejestracji można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129).

14. Kliknij **Zarejestruj**.

Agent dla Synology 6.x

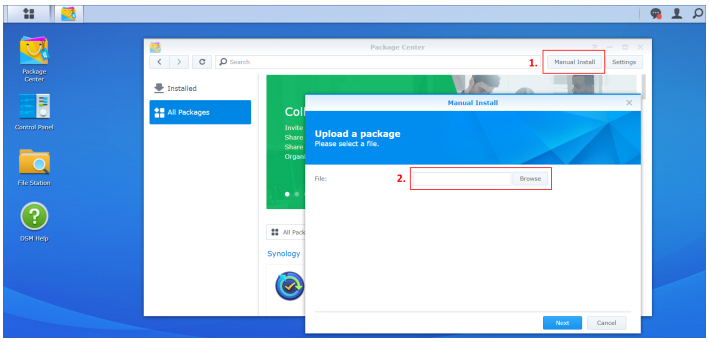
Wymagania wstępne

- Na urządzeniu NAS działa system DiskStation Manager 6.2.x.
- Należysz do grupy **administratorów** na urządzeniu NAS.
- Na woluminie NAS, na którym chcesz zainstalować agenta, jest co najmniej 200 MB wolnego miejsca.

Aby zainstalować agenta dla Synology

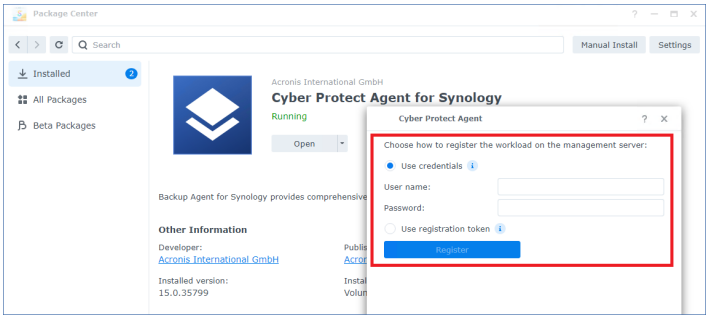
1. Zaloguj się do systemu Synology DiskStation Manager.
2. Otwórz okno **Package Center** (Centrum pakietów).
3. Kliknij **Manual Install** (Instalacja ręczna), a następnie kliknij **Browse** (Przeglądaj).

© Acronis International GmbH, 2003-2024



4. Wybierz plik SPK pobrany z konsoli Cyber Protect, a następnie kliknij **Next** (Dalej).

   Zostanie wyświetlone ostrzeżenie, że jest instalowany pakiet bez podpisu cyfrowego. Komunikat ten stanowi część standardowej procedury instalacji.
5. Aby potwierdzić, że chcesz zainstalować pakiet, kliknij **Yes** (Tak).
6. Wybierz wolumin, na którym chcesz zainstalować agenta, a następnie kliknij **Next** (Dalej).
7. Sprawdź ustawienia i kliknij **Apply** (Zastosuj).
8. W sekcji **Package Center** (Centrum pakietów) systemu Synology DiskStation Manager otwórz narzędzie Cyber Protect Agent for Synology.
9. Wybierz metodę rejestracji.



   - [Aby zarejestrować agenta przy użyciu poświadczeń]
     - W polach **Nazwa użytkownika** i **Hasło** podaj poświadczenia dostępu do konta, na którym będzie zarejestrowany agent. Konto to nie może być kontem administratora partnera.
   - [Aby zarejestrować agenta przy użyciu tokenu rejestracji]
     - W polu **Adres rejestracji** podaj dokładny adres centrum danych. Dokładny adres centrum danych to adres URL widoczny po zalogowaniu się w konsoli Cyber Protect. Na przykład `https://us5-cloud.acronis.com`.

       Uwaga

       Nie używaj formatu URL bez adresu centrum danych. Na przykład nie używaj adresu `https://cloud.acronis.com`.

     - W polu **Token** podaj token rejestracji.

       Dodatkowe instrukcje dotyczące generowania tokenu rejestracji można znaleźć w sekcji "Generowanie tokenu rejestracji" (s. 129).
10. Kliknij **Zarejestruj**.

© Acronis International GmbH, 2003-2024

Po dokonaniu rejestracji urządzenie Synology NAS będzie widoczne w konsoli Cyber Protect na karcie **Urządzenia** > **Sieciowa pamięć masowa (NAS)**.

Aby utworzyć kopię zapasową danych przechowywanych na urządzeniu NAS, zastosuj plan ochrony.

Aktualizowanie agenta dla Synology

Można zaktualizować agenta dla Synology 6.x do nowszej wersji agenta dla Synology 6.x. Można też zaktualizować agenta dla Synology 7.x do nowszej wersji agenta dla Synology 7.x.

Aby zaktualizować agenta, uruchom nowszą wersję programu instalacyjnego w systemie Synology DiskStation Manager. Pierwotna rejestracja agenta, jego ustawienia oraz plany zastosowane do chronionych obciążeń zostaną zachowane.

Uwaga
Agenta nie można zaktualizować z poziomu konsoli Cyber Protect.

Uaktualnienie agenta dla Synology 6.x do agenta dla Synology 7.x jest obsługiwane tylko przez odinstalowanie starszego agenta i zainstalowanie nowszego agenta. W takim przypadku wszystkie plany ochrony zostaną odwołane i trzeba będzie ponownie je zastosować ręcznie.

Agent dla Synology 7.x

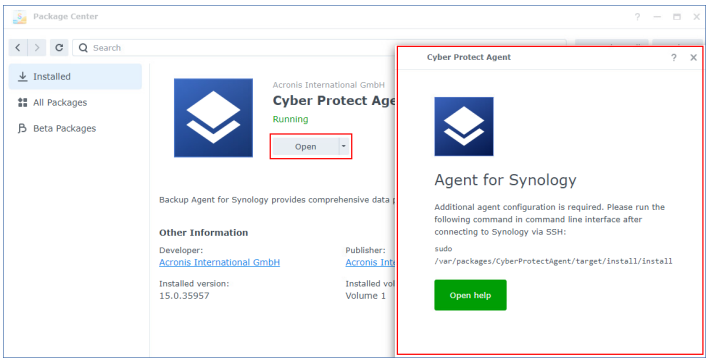
Wymagania wstępne

- Należysz do grupy **administratorów** na urządzeniu NAS.
- Na woluminie NAS, na którym chcesz zainstalować agenta, jest co najmniej 200 MB wolnego miejsca.
- Na komputerze jest dostępny klient SSH. W tym dokumencie na potrzeby przykładu użyto narzędzia Putty.

Aby zaktualizować agenta dla Synology

1. W systemie DiskStation Manager otwórz okno **Package Center** (Centrum pakietów).
2. Kliknij **Manual Install** (Instalacja ręczna), a następnie kliknij **Browse** (Przeglądaj).
3. Wybierz nowszy plik SPK agenta dla Synology 7.x pobrany z konsoli Cyber Protect, a następnie kliknij **Next** (Dalej).
   Zostanie wyświetlone ostrzeżenie, że jest instalowany pakiet oprogramowania innej firmy. Komunikat ten stanowi część standardowej procedury instalacji.
4. Aby potwierdzić, że chcesz zainstalować pakiet, kliknij **Agree** (Zgadzam się).
5. Sprawdź ustawienia i kliknij **Done** (Gotowe).
6. W sekcji **Package Center** (Centrum pakietów) systemu Synology DiskStation Manager otwórz narzędzie Cyber Protect Agent for Synology, a następnie sprawdź, czy jest widoczny następujący ekran.

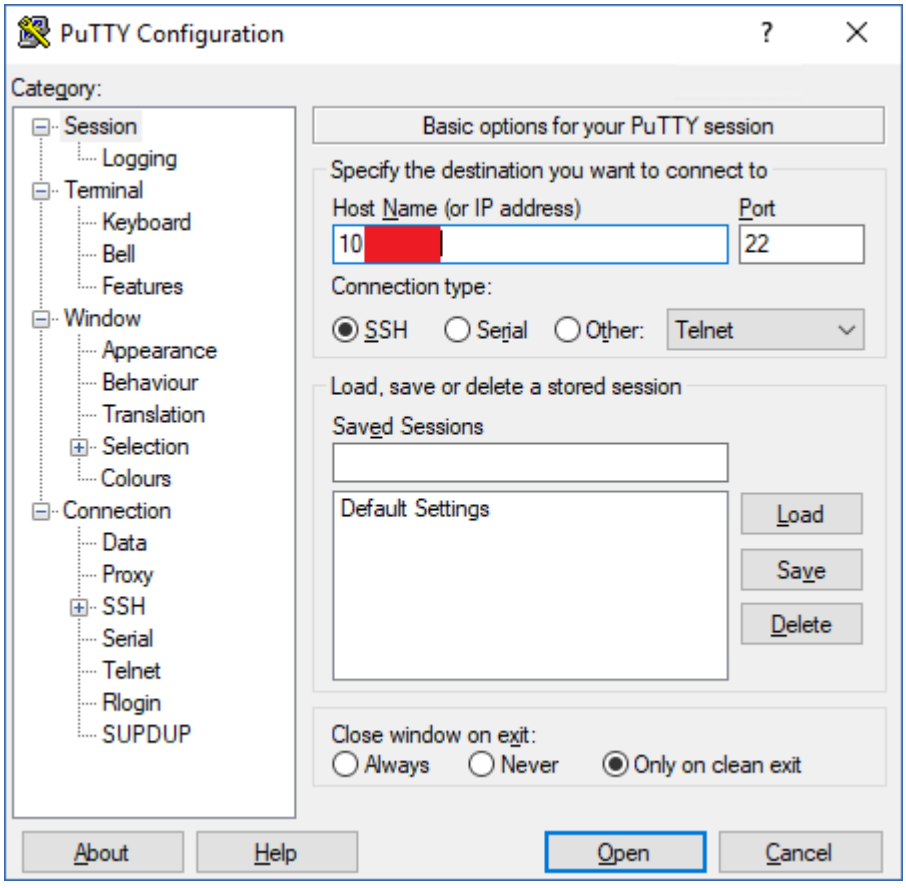
© Acronis International GmbH, 2003-2024



7. W sekcji **Control Panel** (Panel sterowania) systemu Synology DiskStation Manager przejdź do sekcji **Terminal & SNMP** (Terminal i protokół SNMP) i włącz dostęp SSH do urządzenia NAS.
8. Uruchom skrypt `install` na urządzeniu NAS przy użyciu klienta SSH (w tym przykładzie: narzędzia Putty).

   Skrypt ten umożliwia dostęp na poziomie użytkownika root do systemu DSM 7.0 lub nowszego, który jest wymagany do skonfigurowania agenta.

   a. Uruchom narzędzie Putty, a następnie podaj adres IP lub nazwę hosta urządzenia Synology NAS.



   b. Kliknij **Open** (Otwórz) i się zaloguj jako administrator systemu Synology DSM.

   c. Uruchom następujące polecenie.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```


© Acronis International GmbH, 2003-2024

9. W sekcji **Control Panel** (Panel sterowania) systemu Synology DiskStation Manager przejdź do sekcji **Terminal & SNMP** (Terminal i protokół SNMP) i wyłącz dostęp SSH do urządzenia NAS. Dostęp SSH nie jest już wymagany.

Agent dla Synology 6.x

Wymagania wstępne

- Należysz do grupy **administratorów** na urządzeniu NAS.
- Na woluminie NAS, na którym chcesz zainstalować agenta, jest co najmniej 200 MB wolnego miejsca.

Aby zaktualizować agenta dla Synology

1. W systemie DiskStation Manager otwórz okno **Package Center** (Centrum pakietów).
2. Kliknij **Manual Install** (Instalacja ręczna), a następnie kliknij **Browse** (Przeglądaj).
3. Wybierz nowszy plik SPK agenta dla Synology 6.x pobrany z konsoli Cyber Protect, a następnie kliknij **Next** (Dalej).
   Zostanie wyświetlone ostrzeżenie, że jest instalowany pakiet bez podpisu cyfrowego. Komunikat ten stanowi część standardowej procedury instalacji.
4. Aby potwierdzić, że chcesz zainstalować pakiet, kliknij **Yes** (Tak).
5. Sprawdź ustawienia i kliknij **Apply** (Zastosuj).

Połączenia SSH z urządzeniem wirtualnym

Aby uzyskać dostęp zdalny do urządzenia wirtualnego w celu przeprowadzenia prac konserwacyjnych, użyj połączenia Secure Socket Shell (SSH).

Uruchamianie demona Secure Shell

Aby umożliwić połączenia SSH z urządzeniem wirtualnym, uruchom na urządzeniu demona Secure Shell (sshd).

Aby uruchomić demona Secure Shell

1. W oprogramowaniu hiperwizora otwórz konsolę urządzenia wirtualnego.
2. W graficznym interfejsie użytkownika urządzenia naciśnij CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.
3. Uruchom następujące polecenie:

   ```
   /bin/sshd
   ```

4. [Tylko podczas nawiązywania pierwszego połączenia z urządzeniem] Ustaw hasło użytkownika `root`.
   Aby się dowiedzieć, jak ustawić hasło, zobacz "Ustawianie hasła użytkownika root na urządzeniu wirtualnym" (s. 180).

© Acronis International GmbH, 2003-2024

Uwaga
Zalecamy zatrzymanie demona Secure Shell, gdy nie korzystasz z połączenia SSH.

Ustawianie hasła użytkownika root na urządzeniu wirtualnym

Zanim po raz pierwszy nawiążesz połączenie SSH z urządzeniem wirtualnym, musisz ustawić na urządzeniu hasło użytkownika root.

Aby ustawić hasło użytkownika root

1. W oprogramowaniu hiperwizora otwórz konsolę urządzenia wirtualnego.
2. W graficznym interfejsie użytkownika urządzenia naciśnij CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.
3. Uruchom następujące polecenie:

   ```
   passwd
   ```

4. Wpisz hasło, a następnie naciśnij klawisz Enter.

   Hasło musi zawierać co najmniej dziewięć znaków i musi mieć ocenę złożoności na poziomie trzy lub wyższym. Ocena złożoności jest obliczana automatycznie. Aby osiągnąć wyższą ocenę, użyj kombinacji znaków specjalnych, wielkich i małych liter oraz cyfr.
5. Potwierdź hasło, a następnie naciśnij klawisz Enter.

Dostęp do urządzenia wirtualnego za pomocą klienta SSH

Wymagania wstępne

- Klient SSH musi być dostępny na komputerze zdalnym. W poniższej procedurze posłużono się przykładem klienta WinSCP. Możesz użyć dowolnego klienta SSH i tylko odpowiednio dostosować wykonywane kroki.
- Demon Secure Shell (sshd) musi być uruchomiony na urządzeniu wirtualnym. Aby uzyskać więcej informacji, zobacz "Uruchamianie demona Secure Shell" (s. 179).

Aby uzyskać dostęp do urządzenia wirtualnego za pomocą klienta WinSCP

1. Na komputerze zdalnym otwórz klienta WinSCP.
2. Kliknij **Sesja** > **Nowa sesja**.
3. W polu **Protokół plików** wybierz **SCP**.
4. W polu **Nazwa hosta** wpisz adres IP urządzenia wirtualnego.
5. W polach **Nazwa użytkownika** i **Hasło** wpisz `root` i hasło użytkownika `root`.
6. Kliknij **Zaloguj**.

Zostanie wyświetlona lista wszystkich katalogów na urządzeniu wirtualnym.

© Acronis International GmbH, 2003-2024

Automatyczne wykrywanie komputerów

Wykrywanie automatyczne umożliwia:

- Automatyzowanie instalacji agentów ochrony i rejestracji komputerów dzięki funkcji wykrywania komputerów w domenie Active Directory lub sieci lokalnej.
- Instalowanie i aktualizowanie agentów ochrony na wielu komputerach.
- Korzystanie z synchronizacji z domeną Active Directory w celu zmniejszenia nakładu pracy związanej z alokowaniem zasobów i zarządzaniem komputerami w dużej domenie Active Directory.

Wymagania wstępne

- Dostępny musi być co najmniej jeden komputer z zainstalowanym agentem ochrony w sieci lokalnej lub domenie Active Directory. Agent ten będzie używany jako agent wykrywania.
- Musisz mieć przypisaną jedną z następujących ról dla usługi Cyber Protection: Cyberadministrator lub Administrator.

Ważne
Agentami wykrywania mogą być tylko agenty zainstalowane na komputerach z systemem Windows. Jeśli w środowisku nie ma agentów wykrywania, nie będzie można skorzystać z opcji **Wiele urządzeń** w panelu **Dodaj urządzenia**.

Zdalna instalacja agentów jest obsługiwana tylko w przypadku komputerów z systemem Windows (system Windows XP nie jest obsługiwany). Aby dokonać instalacji zdalnej na komputerze z systemem Windows Server 2012 R2, musi na tym komputerze być zainstalowana aktualizacja systemu Windows KB2999226.

Jak działa wykrywanie automatyczne

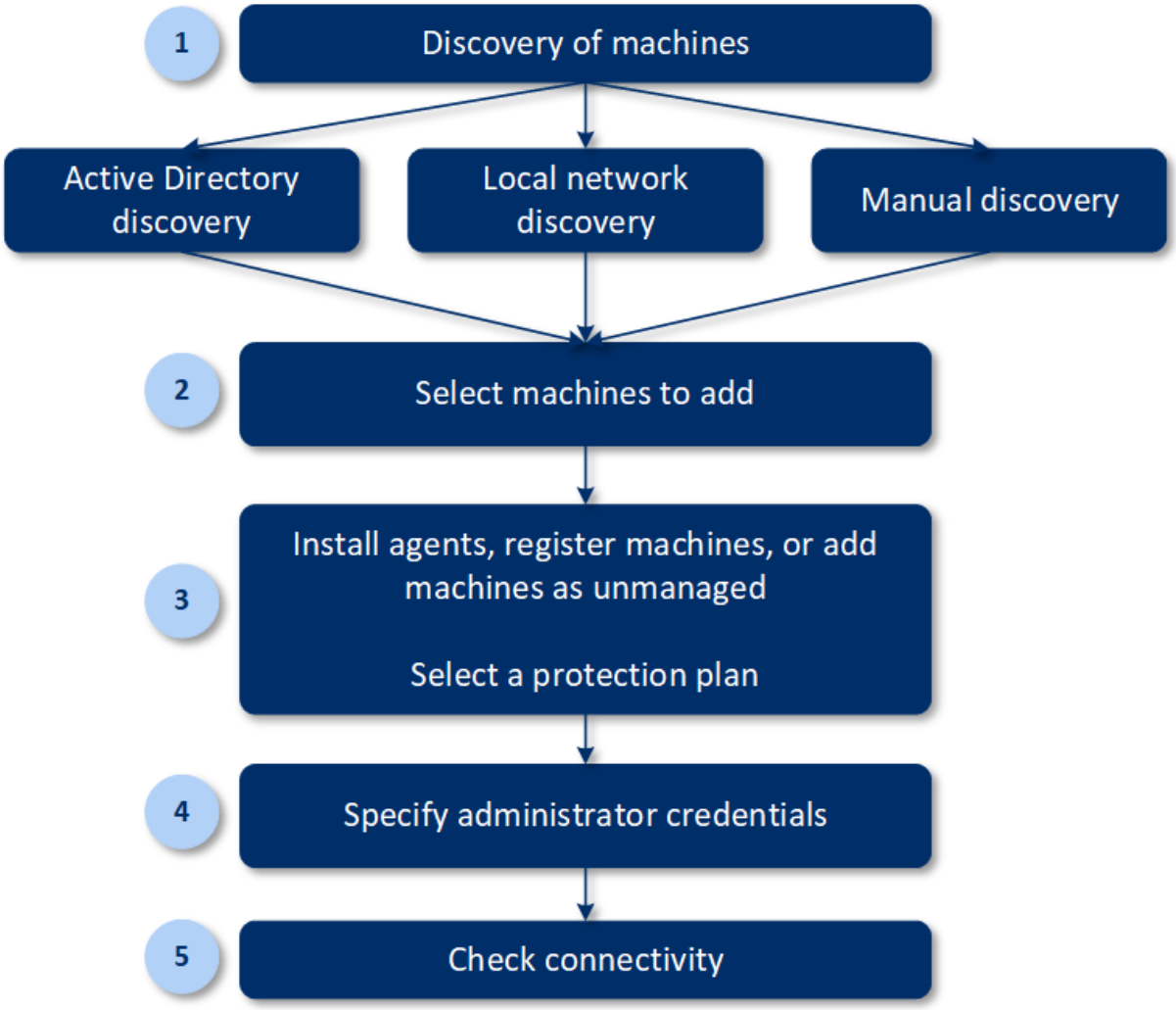
Podczas wykrywania w sieci lokalnej agent wykrywania zbiera następujące informacje na temat każdego komputera w sieci, korzystając z funkcji wykrywania NetBIOS, usługi Web Service Discovery (WSD) oraz tabeli Address Resolution Protocol (ARP):

- Nazwa (nazwa hosta krótka/NetBIOS)
- W pełni kwalifikowana nazwa domeny (FQDN)
- Domena/grupa robocza
- Adres IPv4/IPv6
- Adres MAC
- System operacyjny (nazwa, wersja, rodzina)
- Kategoria komputera (stacja robocza, serwer, kontroler domeny)

© Acronis International GmbH, 2003-2024

Podczas wykrywania w domenie Active Directory agent wykrywania zbiera informacje z powyższej listy, a także informacje nazwy jednostek organizacyjnych komputerów oraz szczegółowe informacje na temat ich nazw i systemów operacyjnych. Adresy IP ani MAC nie są jednak zbierane.

Poniższy diagram stanowi podsumowanie procesu wykrywania automatycznego.



1. Wybierz metodę wykrywania:
   - Wykrywanie w domenie Active Directory
   - Wykrywanie w sieci lokalnej
   - Wykrywanie ręczne — za pomocą adresu IP lub nazwy hosta komputera albo przez zaimportowanie listy komputerów z pliku

   Wyniki wykrywania w domenie Active Directory lub sieci lokalnej nie obejmują komputerów z zainstalowanymi agentami ochrony.

   W przypadku wykrywania ręcznego istniejące agenty ochrony są aktualizowane i ponownie rejestrowane. W przypadku wykrywania automatycznego przy użyciu tego samego konta, na którym jest zarejestrowany agent, agent zostanie tylko zaktualizowany do najnowszej wersji. W przypadku wykrywania automatycznego przy użyciu innego konta agent zostanie zaktualizowany do najnowszej wersji i ponownie zarejestrowany w ramach dzierżawcy, do którego należy konto.

© Acronis International GmbH, 2003-2024

2. Wybierz komputery, które chcesz dodać do dzierżawcy.
3. Wybierz, jak mają zostać dodane te komputery:
   - Zainstaluj agenta ochrony i dodatkowe komponenty na tych komputerach oraz zarejestruj je w konsoli Cyber Protect.
   - Zarejestruj komputery w konsoli Cyber Protect (jeśli agent ochrony został już zainstalowany).
   - Dodaj komputery do konsoli Cyber Protect jako **Komputery niezarządzane** bez instalowania agenta ochrony.

   Możesz też zastosować już istniejący plan ochrony do komputerów, na których jest instalowany agent ochrony lub które są rejestrowane w konsoli Cyber Protect.
4. Podaj poświadczenia administratora dla wybranych komputerów.
5. Sprawdź, czy możesz nawiązać połączenie z tymi komputerami przy użyciu podanych poświadczeń.

Komputery widoczne w konsoli Cyber Protect zaliczają się do następujących kategorii:

- **Wykryte** — komputery, które zostały wykryte, ale nie mają zainstalowanego agenta ochrony.
- **Zarządzane** — komputery z zainstalowanym agentem ochrony.
- **Niechronione** — komputery, do których nie zastosowano planu ochrony. W grupie niechronionych komputerów są uwzględniane zarówno wykryte, jak i zarządzane komputery, do których nie zastosowano planu ochrony.
- **Chronione** — komputery, do których zastosowano plan ochrony.

Jak działa zdalna instalacja agentów

1. Agent wykrywania łączy się z komputerami docelowymi przy użyciu nazw hostów, adresów IP i poświadczeń administratora podanych w kreatorze wykrywania, a następnie przesyła na te komputery plik `web_installer.exe`.
2. Plik `web_installer.exe` zostaje uruchomiony na komputerach docelowych w trybie nienadzorowanym.
3. Instalator internetowy pobiera z chmury dodatkowe pakiety instalacyjne, a następnie instaluje je na komputerach docelowych za pomocą polecenia `msiexec`.
4. Po zakończeniu instalacji komponenty są rejestrowane w chmurze.

Uwaga
W przypadku kontrolerów domen instalacja zdalna agentów nie jest obsługiwana z powodu dodatkowych uprawnień wymaganych do uruchomienia usługi agenta.

Wykonywanie automatycznego i ręcznego wykrywania

Przed rozpoczęciem operacji wykrywania upewnij się, że zostały spełnione wymagania wstępne.

© Acronis International GmbH, 2003-2024

Uwaga
W przypadku dodawania kontrolerów domen wykrywanie automatyczne nie jest obsługiwane z powodu dodatkowych uprawnień wymaganych do uruchomienia usługi agenta.

Aby wykryć komputery

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij **Dodaj**.
3. W obszarze **Wiele urządzeń** kliknij **Tylko Windows**. Zostanie uruchomiony Kreator wykrywania automatycznego.
4. [Jeśli w organizacji są jednostki] Wybierz jednostkę. Wówczas w polu **Agent wykrywania** będzie można wybrać agenty związane z wybraną jednostką i jej jednostkami podrzędnymi.
5. Wybierz agenta wykrywania, który ma przeprowadzić skanowanie w celu wykrycia komputerów.
6. Wybierz metodę wykrywania:
   - **Szukaj w usłudze Active Directory**. Upewnij się, że komputer z agentem wykrywania należy do domeny Active Directory.
   - **Skanuj sieć lokalną**. Jeśli wybrany agent wykrywania nie znalazł żadnego komputera, wybierz innego agenta wykrywania.
   - **Wpisz ręcznie lub zaimportuj z pliku**. Ręcznie zdefiniuj komputery, które mają zostać dodane, lub zaimportuj je z pliku tekstowego.
7. [Jeśli wybrano metodę wykrywania w domenie Active Directory] Wybierz sposób wyszukiwania komputerów:
   - **Na liście jednostek organizacyjnych**. Wybierz grupę komputerów, które mają zostać dodane.
   - **Według zapytania w dialekcie LDAP**. Użyj zapytania w dialekcie LDAP, aby wybrać komputery. Opcja **Baza wyszukiwania** umożliwia określenie przeszukiwanych miejsc, a pole **Filtruj** umożliwia podanie kryteriów wyboru komputerów.

© Acronis International GmbH, 2003-2024

8. W zależności od wybranej metody wykrywania wykonaj jedną z następujących czynności:

Metoda wykrywania	Czynność
Szukaj w usłudze Active Directory	Z listy wykrytych komputerów wybierz te, które chcesz dodać.
Skanuj sieć lokalną	Z listy wykrytych komputerów wybierz te, które chcesz dodać.

Wpisz ręcznie lub zaimportuj z pliku	Podaj adresy IP lub nazwy hostów komputerów albo zaimportuj listę komputerów z pliku tekstowego. Plik musi zawierać adresy IP / nazwy hostów zapisane po jednym w każdym wierszu. Oto przykładowy plik:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Po ręcznym dodaniu adresów komputerów lub zaimportowaniu ich z pliku agent próbuje wysłać do dodanych komputerów polecenia ping i ustalić ich dostępność.

9. Wybierz czynności, które muszą zostać podjęte po wykryciu:

Opcja	Opis
Zainstaluj agenty i zarejestruj komputery	Możesz wybrać komponenty, które mają zostać zainstalowane na komputerach, klikając **Wybierz komponenty**. Dodatkowe informacje można znaleźć w sekcji "Wybieranie komponentów do zainstalowania" (s. 189).
Konto logowania dla usługi agenta	To ustawienie jest dostępne na ekranie **Wybierz komponenty**. Ustawienie określa konto, w ramach którego będą uruchamiane usługi. Możesz wybrać jedną z następujących opcji: • **Użyj kont użytkowników usługi** (domyślne w przypadku usługi agenta) Konta użytkowników usługi to konta w systemie Windows używane do uruchamiania usług. Ustawienie to ma tę zaletę, że zasady zabezpieczeń domeny nie wpływają na prawa użytkowników tych kont. Domyślnie agent działa na koncie **System lokalny**. • **Utwórz nowe konto** Nazwą konta dla danego agenta będzie Agent User. • **Użyj następującego konta** Jeśli agent zostanie zainstalowany na kontrolerze domeny, system wyświetli monit o określenie istniejących już kont (lub tego samego konta) na potrzeby agenta. Ze względów bezpieczeństwa system nie tworzy automatycznie nowych kont na kontrolerze domeny. W przypadku wybrania opcji **Utwórz nowe konto** lub **Użyj następującego**

© Acronis International GmbH, 2003-2024

Opcja	Opis
	konta dopilnuj, aby zasady zabezpieczeń domeny nie wpływały na prawa powiązanych kont. Jeśli konto straci prawa użytkownika przypisane podczas instalacji, komponent może działać niepoprawnie lub wcale nie działać.
Zarejestruj komputery z zainstalowanymi agentami	Użyj tej opcji, jeśli agent jest już zainstalowany na komputerach i wystarczy je tylko zarejestrować Cyber Protection. W przypadku nieznalezienia na komputerach żadnego agenta zostaną one dodane jako komputery **Niezarządzane**.
Dodaj jako komputery niezarządzane	W przypadku wybrania tej opcji agent nie zostanie zainstalowany na tych komputerach. Będzie można je przeglądać w konsoli i zainstalować lub zarejestrować agenta później.
W razie potrzeby uruchom ponownie komputer	Ta opcja jest widoczna, gdy została wybrana opcja **Zainstaluj agenty i zarejestruj komputery**. W przypadku wybrania tej opcji komputer zostanie uruchomiony ponownie tyle razy, ile będzie konieczne w celu ukończenia instalacji. Ponowne uruchomienie komputera może być wymagane w jednym z poniższych przypadków: • Ukończono instalację oprogramowania określonego w wymaganiach wstępnych instalacji i trzeba uruchomić ponownie komputer, aby kontynuować instalację. • Ukończono instalację, ale trzeba uruchomić ponownie komputer, ponieważ niektóre pliki zostały zablokowane na czas instalacji. • Ukończono instalację, ale trzeba uruchomić ponownie komputer ze względu na inne wcześniej zainstalowane oprogramowanie.
Nie uruchamiaj ponownie, jeśli jest zalogowany użytkownik	Ta opcja jest widoczna, gdy została wybrana opcja **W razie potrzeby uruchom ponownie komputer**. W przypadku wybrania tej opcji komputer nie zostanie automatycznie uruchomiony ponownie, jeśli użytkownik jest zalogowany w systemie. Jeśli na przykład użytkownik pracuje, gdy instalacja wymaga ponownego uruchomienia, system nie zostanie uruchomiony ponownie. Jeśli wymagane oprogramowanie zostało zainstalowane, ale komputer nie został uruchomiony ponownie ze względu na zalogowaną sesję użytkownika, to w celu ukończenia instalacji należy uruchomić ponownie komputer, a potem jeszcze raz rozpocząć instalację. Jeśli agent został zainstalowany, ale komputer nie został uruchomiony ponownie, należy uruchomić ponownie komputer.
Użytkownik, w ramach którego mają zostać zarejestrowane komputery	[Jeśli organizacja ma jednostki] Wybierz konto użytkownika z jednostki lub jednostek podrzędnych, w ramach którego mają zostać zarejestrowane komputery. [W przypadku wykonywania wykrywania automatycznego na poziomie dzierżawcy-partnera] Na liście dzierżawców-klientów, którymi zarządzasz,

© Acronis International GmbH, 2003-2024

Opcja	Opis
	rozwiń strukturę drzewa, a następnie wybierz konto użytkownika, w ramach którego chcesz zarejestrować komputery. [W przypadku wykonywania wykrywania automatycznego jako administrator klienta] Jeśli została wybrana opcja **Zainstaluj agenty i zarejestruj komputery** lub **Zarejestruj komputery z zainstalowanymi agentami**, dostępna jest też możliwość zastosowania planu ochrony do komputerów. Jeśli masz kilka planów ochrony, możesz wybrać, którego chcesz użyć.

10. Podaj poświadczenia użytkownika, który ma prawa administratora do wszystkich dodanych komputerów.

Ważne
Należy pamiętać, że zdalna instalacja agenta działa bez żadnych przygotowań tylko w przypadku podania poświadczeń dostępu do wbudowanego konta administratora (pierwszego konta utworzonego podczas instalacji systemu operacyjnego). Aby zdefiniować poświadczenia dla niestandardowego administratora, należy wykonać dodatkowe przygotowania ręczne, zgodnie z opisem podanym w sekcji "Przygotowywanie komputera do instalacji zdalnej" (s. 187).

11. System sprawdza możliwość nawiązania połączenia ze wszystkimi komputerami. Jeśli w przypadku jakichś komputerów połączenie się nie powiedzie, można zmienić dotyczące ich poświadczenia.

Po zainicjowaniu operacji wykrywania komputerów odpowiednie zadanie można znaleźć w działaniu **Monitorowanie** > **Działania** > **Wykrywanie komputerów**.

Przygotowywanie komputera do instalacji zdalnej

- Aby można było pomyślnie przeprowadzić instalację na komputerze zdalnym z systemem Windows 7 lub nowszym, musi na nim być wyłączona opcja **Panel sterowania** > **Opcje folderów** > **Widok** > **Użyj Kreatora udostępniania**.
- Aby pomyślnie przeprowadzić instalację na komputerze zdalnym, który *nie* należy do domeny Active Directory, musi na nim być *wyłączona* funkcja Kontrola konta użytkownika (UAC). Więcej informacji na temat wyłączania tej funkcji można znaleźć w sekcji „Wymagania dotyczące funkcji Kontrola konta użytkownika (UAC)” > Aby wyłączyć funkcję UAC.
- Domyślnie do instalacji na dowolnym zdalnym komputerze z systemem Windows są wymagane poświadczenia dostępu do wbudowanego konta administratora. Aby przeprowadzić instalację zdalną przy użyciu poświadczeń dostępu do innego konta administratora, należy *wyłączyć* ograniczenia funkcji UAC dotyczące połączeń zdalnych. Więcej informacji na temat ich wyłączania można znaleźć w sekcji „Wymagania dotyczące funkcji Kontrola konta użytkownika (UAC)” > Aby wyłączyć ograniczenia funkcji UAC dotyczące połączeń zdalnych.
- Na komputerze zdalnym należy *włączyć* udostępnianie plików i drukarek. Aby uzyskać dostęp do tej opcji:

© Acronis International GmbH, 2003-2024

- Na komputerze z systemem lub Windows 2003 Server: wybierz **Panel sterowania** > **Zapora systemu Windows** > **Wyjątki** > **Udostępnianie plików i drukarek**.
- Na komputerze z systemem Windows Server 2008, Windows 7 lub nowszym: wybierz **Panel sterowania** > **Zapora systemu Windows** > **Centrum sieci i udostępniania** > **Zmień zaawansowane ustawienia udostępniania**.

- Usługa Cyber Protection używa do instalacji zdalnej portów TCP 445, 25001 i 43234.

  Port 445 jest automatycznie otwierany po wybraniu opcji Udostępnianie plików i drukarek. Porty 43234 i 25001 są automatycznie otwierane przez Zaporę systemu Windows. W przypadku korzystania z innej zapory sprawdź, czy porty te są otwarte (dodane do listy wyjątków) zarówno dla żądań przychodzących, jak i wychodzących.

  Po zakończeniu instalacji zdalnej port 25001 jest automatycznie zamykany przez Zaporę systemu Windows. Jeśli chcesz aktualizować agenta zdalnie w przyszłości, porty 445 i 43234 muszą pozostać otwarte. Przy każdej aktualizacji port 25001 jest automatycznie ponownie otwierany i zamykany przez Zaporę systemu Windows. W przypadku korzystania z innej zapory sieciowej wszystkie trzy porty pozostaną otwarte.

Wymagania dotyczące funkcji Kontrola konta użytkownika (UAC)

Na komputerze z systemem operacyjnym Windows 7 lub nowszym, który nie należy do domeny Active Directory, trzeba wyłączyć funkcję Kontrola konta użytkownika (UAC) i jej ograniczenia dotyczące połączeń zdalnych, aby zapewnić prawidłowy przebieg operacji zarządzania scentralizowanego (w tym instalacji zdalnej).

Aby wyłączyć funkcję UAC

Zależnie od wersji systemu operacyjnego wykonaj jedną z następujących czynności:

- **W systemie operacyjnym Windows starszym niż Windows 8:**

  Przejdź do sekcji **Panel sterowania > Widok: Małe ikony > Konta użytkowników > Zmień ustawienia funkcji Kontrola konta użytkownika**, a następnie przesuń suwak w położenie **Nie powiadamiaj nigdy**. Następnie uruchom ponownie komputer.
- **W każdym systemie operacyjnym Windows**:
  1. Uruchom Edytor rejestru.
  2. Odszukaj następujący klucz rejestru: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Zmień wartość **EnableLUA** na **0**.
  4. Uruchom ponownie komputer.

Aby wyłączyć ograniczenia funkcji UAC dotyczące połączeń zdalnych

1. Uruchom Edytor rejestru.
2. Odszukaj następujący klucz rejestru: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Zmień wartość **LocalAccountTokenFilterPolicy** na **1**.

© Acronis International GmbH, 2003-2024

Jeśli wartość **LocalAccountTokenFilterPolicy** nie istnieje, utwórz ją jako DWORD (32-bitowy). Dodatkowe informacje na temat tej wartości można znaleźć w dokumentacji firmy Microsoft: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Uwaga
Ze względów bezpieczeństwa zalecamy przywrócenie — po zakończeniu operacji zarządzania (np. instalacji zdalnej) — obu ustawień do stanu pierwotnego: **EnableLUA**=**1** i **LocalAccountTokenFilterPolicy** = **0**

Wybieranie komponentów do zainstalowania

Poniższa tabela zawiera opisy wymaganych i dodatkowych komponentów:

Komponent	Opis
Wymagany komponent	
Agent dla systemu Windows	Ten agent tworzy kopie zapasowe dysków, woluminów i plików. Jest instalowany na komputerach z systemem Windows. Zawsze zostanie zainstalowany — brak możliwości wyboru.
Dodatkowe komponenty	
Agent dla rozwiązania Data Loss Prevention	Ten agent umożliwia ograniczenie dostępu użytkowników do lokalnych oraz przekierowywanych urządzeń peryferyjnych, portów i schowka na komputerach objętych planami ochrony. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Ochrona przed złośliwym oprogramowaniem i filtrowanie adresów URL	Ten komponent powoduje udostępnienie modułu Ochrona przed wirusami i złośliwym oprogramowaniem oraz modułu Filtrowanie adresów URL w planach ochrony. Nawet jeśli nie zainstalujesz tego komponentu, zostanie on automatycznie zainstalowany później, jeśli któryś z wymienionych modułów zostanie włączony w planie ochrony komputera.
Agent dla Hyper-V	Ten agent tworzy kopie zapasowe maszyn wirtualnych Hyper-V. Jest instalowany na hostach Hyper-V. Zostanie zainstalowany w przypadku wybrania takiej opcji i wykrycia na komputerze roli Hyper-V.
Agent dla SQL	Ten agent tworzy kopie zapasowe baz danych programu SQL Server. Jest instalowany na komputerach z programem Microsoft SQL Server. Zostanie zainstalowany w przypadku wybrania takiej opcji i wykrycia programu na komputerze.
Agent dla programu Exchange	Ten agent tworzy kopie zapasowe baz danych programu Exchange. Jest instalowany na komputerach z rolą Skrzynka pocztowa programu Microsoft Exchange Server. Zostanie zainstalowany w przypadku wybrania takiej opcji i wykrycia programu na komputerze.
Agent dla usługi	Ten agent tworzy kopie zapasowe danych Usług domenowych Active Directory.

© Acronis International GmbH, 2003-2024

Active Directory	Jest instalowany na kontrolerach domen. Zostanie zainstalowany w przypadku wybrania takiej opcji i wykrycia programu na komputerze.
Agent dla VMware (Windows)	Ten agent tworzy kopie zapasowe maszyn wirtualnych VMware. Jest instalowany na komputerach z systemem Windows, które mają dostęp sieciowy do serwera vCenter. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Agent dla usługi Microsoft 365	Ten agent tworzy kopie zapasowe skrzynek pocztowych pakietu Microsoft 365 w lokalnym miejscu docelowym. Jest instalowany na komputerach z systemem Windows. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Agent dla programu Oracle	Ten agent tworzy kopie zapasowe baz danych Oracle. Jest instalowany na komputerach z oprogramowaniem Oracle Database. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Cyber Protection Monitor	Ten komponent umożliwia użytkownikowi monitorowanie wykonywania uruchomionych zadań w obszarze powiadomień. Jest instalowany na komputerach z systemem Windows. Zostanie zainstalowany w przypadku wybrania takiej opcji. Jest obsługiwany w systemach Windows 7 z dodatkiem Service Pack 1 lub nowszym i Windows Server 2008 R2 z dodatkiem Service Pack 1 lub nowszym.

Zarządzanie wykrytymi komputerami

Po zakończeniu procesu wykrywania wszystkie wykryte komputery można znaleźć w sekcji **Urządzenia** > **Komputery niezarządzane**.

Sekcja ta jest podzielona na podsekcje według zastosowanej metody wykrywania. Oto pełna lista parametrów komputerów (mogą być różne w zależności od metody wykrywania):

Nazwa	Opis
Nazwa	Nazwa komputera. Jeśli nie wykryto nazwy komputera, będzie wyświetlany jego adres IP.
Adres IP	Adres IP komputera.
Typ wykrywania	Metoda wykrywania zastosowana w celu wykrycia maszyny.
Jednostka organizacyjna	Jednostka organizacyjna w domenie Active Directory, do której należy komputer. Ta kolumna jest wyświetlana w przypadku przeglądania listy komputerów w sekcji **Komputery niezarządzane** > **Active Directory**.
System operacyjny	System operacyjny zainstalowany na komputerze.

W sekcji **Wyjątki** można dodać komputery, które mają zostać pominięte podczas wykrywania. Jeśli na przykład nie potrzebujesz, być któreś komputery zostały wykryte, możesz je dodać do tej listy.

© Acronis International GmbH, 2003-2024

Aby dodać komputer w sekcji **Wyjątki**, zaznacz go na liście i kliknij **Dodaj do wyjątków**. Aby usunąć komputer z sekcji **Wyjątki**, przejdź do sekcji **Komputery niezarządzane** > **Wyjątki**, zaznacz komputer i kliknij **Usuń z wyjątków**.

Możesz zainstalować agenta ochrony i zarejestrować grupę wykrytych komputerów w usłudze Cyber Protection — w tym celu zaznacz je na liście i kliknij **Zainstaluj i zarejestruj**. Otwarty kreator pozwala również na przypisanie planu ochrony do grupy komputerów.

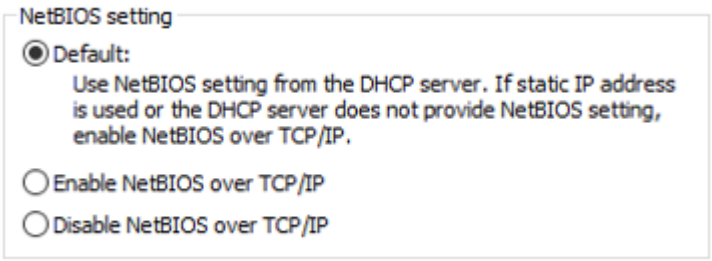
Po zainstalowaniu na komputerach agenta ochrony komputery te będą widoczne w sekcji **Urządzenia** > **Komputery z agentami**.

Aby sprawdzić status ochrony, przejdź do sekcji **Monitorowanie** > **Przegląd** i dodaj widżet **Status ochrony** lub **Wykryty komputer**.

Rozwiązywanie problemów

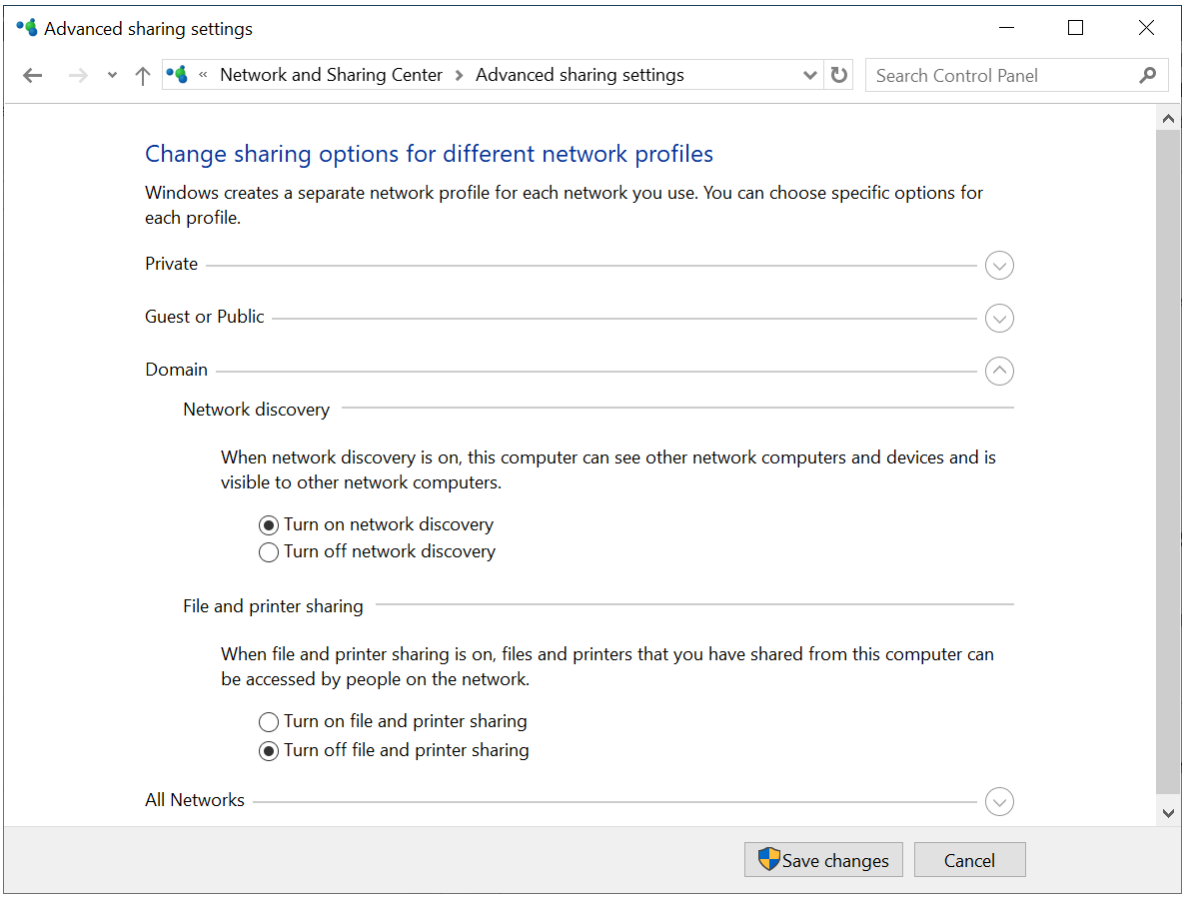
W razie jakichkolwiek problemów z funkcją automatycznego wykrywania spróbuj podjąć następujące kroki:

- Sprawdź, czy jest włączony lub ustawiony jako domyślny protokół NetBIOS over TCP/IP.



- W sekcji „Panel sterowania\Centrum sieci i udostępniania\Zaawansowane ustawienia udostępniania” włącz Odnajdowanie sieci.

© Acronis International GmbH, 2003-2024



- Sprawdź, czy na komputerze obsługującym wykrywanie oraz komputerach, które mają zostać wykryte, działa usługa Host dostawcy odnajdowania funkcji.
- Sprawdź, czy na komputerach, które mają zostać wykryte, działa usługa Publikacja zasobów odnajdowania funkcji.

Zapobieganie nieuprawnionym dezinstalacjom lub modyfikacjom agentów

Agenta dla systemu Windows można chronić przed nieuprawnioną dezinstalacją lub modyfikacją, włączając ustawienie **Ochrona hasłem** w planie ochrony. To ustawienie jest dostępne tylko wtedy, gdy jest włączone ustawienie **Ochrona własna**.

Aby włączyć ochronę hasłem

1. W planie ochrony rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem** (moduł **Active Protection** w wersjach Cyber Backup).
2. Kliknij **Ochrona własna** i upewnij się, że przełącznik **Ochrona własna** jest włączony.
3. Włącz przełącznik **Ochrona hasłem**.
4. W nowo otwartym oknie skopiuj hasło, które jest potrzebne do odinstalowania lub zmodyfikowania komponentów chronionego agenta dla systemu Windows.

© Acronis International GmbH, 2003-2024

Hasło jest unikatowe i nie będzie można go odzyskać po zamknięciu okna. Jeśli je zgubisz lub zapomnisz, możesz edytować plan ochrony i utworzyć nowe hasło.

5. Kliknij **Zamknij**.
6. W okienku **Ochrona własna** kliknij **Gotowe**.
7. Zapisz plan ochrony.

Ochrona hasłem zostanie włączona w przypadku komputerów, do których jest stosowany ten plan ochrony. Ochrona hasłem jest dostępna tylko w przypadku agenta dla systemu Windows w wersji *15.0.25851* lub nowszej. Komputery te muszą być w trybie online.

Plan ochrony z włączoną ochroną hasłem można zastosować do komputera z systemem macOS, ale ochrona nie zostanie zapewniona. Takiego planu nie można zastosować do komputera z systemem Linux.

Nie można też zastosować więcej niż jednego planu ochrony z włączoną ochroną hasłem do tego samego komputera z systemem Windows. Informacje na temat usuwania ewentualnych konfliktów można znaleźć w sekcji Usuwanie konfliktów między planami.

Aby zmienić hasło w już istniejącym planie ochrony

1. W planie ochrony rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem** (moduł **Active Protection** w wersji Cyber Backup).
2. Kliknij **Ochrona własna**.
3. Kliknij **Utwórz nowe hasło**.
4. W nowo otwartym oknie skopiuj hasło, które jest potrzebne do odinstalowania lub zmodyfikowania komponentów chronionego agenta dla systemu Windows.
   Hasło jest unikatowe i nie będzie można go odzyskać po zamknięciu okna. Jeśli je zgubisz lub zapomnisz, możesz edytować plan ochrony i utworzyć nowe hasło.
5. Kliknij **Zamknij**.
6. W okienku **Ochrona własna** kliknij **Gotowe**.
7. Zapisz plan ochrony.

Zmienianie limitów usług komputerów

Limit usług jest przypisywany automatycznie w chwili pierwszego zastosowania planu ochrony do komputera.

Przypisywany jest najbardziej odpowiedni limit — z uwzględnieniem typu chronionego komputera, jego systemu operacyjnego, wymaganego poziomu ochrony i dostępności limitu. Jeśli najbardziej odpowiedni limit nie jest dostępny w danej organizacji, przypisywany jest drugi w kolejności spośród najbardziej odpowiednich. Jeśli na przykład najbardziej odpowiednim limitem jest **Serwer hostingu witryn internetowych**, ale nie jest on dostępny, zostanie przypisany limit **Serwer**.

Przykłady przypisania limitów:

© Acronis International GmbH, 2003-2024

- Komputerowi fizycznemu z systemem operacyjnym Windows Server lub Linux (np. Ubuntu Server) zostanie przypisany limit **Serwer**.
- Komputerowi fizycznemu z systemem operacyjnym Windows lub Linux w wersji dla komputerów stacjonarnych (np. Ubuntu Desktop) zostanie przypisany limit **Stacja robocza**.
- Komputerowi fizycznemu z systemem operacyjnym Windows 10 z włączoną rolą Hyper-V zostanie przypisany limit **Stacja robocza**.
- Komputerowi działającemu w ramach infrastruktury VDI, której agent ochrony jest zainstalowany w systemie operacyjnym gościa (np. agent dla systemu Windows), zostanie przypisany limit **Maszyna wirtualna**. Może też zostać zastosowany limit **Stacja robocza**, jeśli limit **Maszyna wirtualna** jest niedostępny.
- Komputerowi działającemu w ramach infrastruktury VDI i uwzględnianemu w kopii zapasowej w trybie bezagentowym (np. za pomocą agenta dla VMware lub agenta dla Hyper-V), zostanie przypisany limit **Maszyna wirtualna**.
- Serwerowi Hyper-V lub vSphere zostanie przypisany limit **Serwer**.
- Serwerowi z panelem sterowania cPanel lub Plesk zostanie przypisany limit **Serwer hostingu witryn internetowych**. W tym przypadku może też zostać zastosowany limit **Maszyna wirtualna** lub **Serwer** — w zależności od typu maszyny, na której działa serwer witryn internetowych — jeśli limit **Serwer hostingu witryn internetowych** jest niedostępny.
- Kopia zapasowa uwzględniająca aplikacje wymaga limitu **Serwer**, nawet w przypadku stacji roboczej.

Później można ręcznie zmienić pierwotne przypisanie. Aby na przykład zastosować bardziej zaawansowany plan ochrony do tego samego komputera, może być konieczne podwyższenie limitu usług komputera. Jeśli funkcje wymagane przez ten plan ochrony nie są obsługiwane przez aktualnie przypisany limit usług, wykonanie planu ochrony się nie powiedzie.

Jeśli po przypisaniu pierwotnego limitu zostanie wykupiony bardziej odpowiedni limity usług, można go zmienić. Załóżmy, że do maszyny wirtualnej został przypisany limit **Stacja robocza**. Po wykupieniu limitu **Maszyny wirtualne** można go ręcznie przypisać do tej maszyny, zastępując pierwotny limit **Stacja robocza**.

Można też zwolnić aktualnie przypisany limit usług i przypisać go do innego komputera lub maszyny wirtualnej.

Istnieje możliwość zmiany limitu usług dla jednego komputera lub maszyny wirtualnej bądź grupy komputerów lub maszyn.

Aby zmienić limit usług dla wybranego komputera

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Wybierz właściwy komputer i kliknij **Szczegóły**.
3. W sekcji **Limit usług** kliknij **Zmień**.
4. W oknie **Zmień limit** wybierz odpowiedni limit usług lub opcję **Brak limitu** i kliknij **Zmień**.

Aby zmienić limit usług dla grupy komputerów

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Wybierz więcej niż jeden komputer i kliknij **Przypisz limit**.
3. W oknie **Zmień limit** wybierz odpowiedni limit usług lub opcję **Brak limitu** i kliknij **Zmień**.

Ustawienia ochrony

Aby skonfigurować ogólne ustawienia ochrony rozwiązania Cyber Protection, w konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Ochrona**.

Automatyczne aktualizacje komponentów

Domyślnie wszystkie agenty mogą się łączyć z Internetem i pobierać aktualizacje.

Administrator może zminimalizować ruch na łączu sieciowym, wybierając w środowisku co najmniej jednego agenta i przypisując mu rolę Aktualizatora. W związku z tym tylko tak wyznaczone agenty będą się łączyć z Internetem i pobierać aktualizacje. Pozostałe agenty będą się łączyć z tymi wyznaczonymi agentami aktualizującymi przy użyciu technologii peer-to-peer i od nich pobierać aktualizacje.

Agenty, które nie mają przypisanej roli Aktualizator, będą się łączyć z Internetem, jeśli w środowisku nie będzie wyznaczonego agenta-aktualizatora lub jeśli przez około 5 minut nie uda się nawiązać połączenia z wyznaczonym agentem-aktualizatorem.

Agent z rolą Aktualizator dystrybuuje aktualizacje i poprawki modułów Ochrona przed wirusami i złośliwym oprogramowaniem, Ocena luk w zabezpieczeniach i Zarządzanie poprawkami, ale nie obejmuje to aktualizacji wersji agentów.

Uwaga
Agent mający rolę Aktualizator może pobierać i dystrybuować poprawki tylko w przypadku produktów innych firm przeznaczonych dla systemu Windows. W przypadku produktów firmy Microsoft dystrybucja poprawek nie jest obsługiwana przez agenta z rolą Aktualizator.

Zanim przypiszesz agentowi rolę Aktualizator, dopilnuj, aby komputer, na którym działa dany agent, był wystarczająco wydajny, miał stabilne, szybkie połączenie z Internetem oraz wystarczającą ilość miejsca na dysku.

Aby przygotować komputer do roli Aktualizator

1. Na komputerze, na którym ma zostać włączona rola Aktualizator, należy zastosować następujące reguły zapory sieciowej:
   - Ruch przychodzący „updater_incoming_tcp_ports”: zezwól na połączenia przy użyciu portów TCP 18018 i 6888 dla wszystkich profili zapory (publicznego, prywatnego i domeny).
   - Ruch przychodzący „updater_incoming_udp_ports”: zezwól na połączenia przy użyciu portu UDP 6888 dla wszystkich profili zapory (publicznego, prywatnego i domeny).
2. Uruchom ponownie usługę Acronis Agent Core Service.
3. Uruchom ponownie usługę zapory.

© Acronis International GmbH, 2003-2024

Jeśli te reguły nie zostaną zastosowane, a zapora jest włączona, agenty równorzędne będą pobierać aktualizacje z magazynu Cloud.

Aby przypisać rolę aktualizatora do agenta ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Wybierz komputer z agentem, do którego chcesz przypisać rolę aktualizatora.
3. Kliknij **Szczegóły** i włącz przełącznik **Użyj tego agenta, aby pobrać oraz rozpowszechnić poprawki i aktualizacje**.

Aktualizacje peer-to-peer działają następująco.

1. Agent z rolą aktualizatora sprawdza — zgodnie z harmonogramem — plik indeksu udostępniany przez dostawcę usługi w celu aktualizacji głównych komponentów.
2. Agent z rolą aktualizatora zaczyna pobierać aktualizacje i je rozpowszechniać wśród wszystkich agentów.

Rolę Aktualizator można przypisać do wielu agentów w środowisku. Dzięki temu w sytuacji, gdy agent mający przypisaną rolę Aktualizator jest offline, inne agenty z tą rolą mogą służyć jako źródła aktualizacji definicji.

Aktualizowanie definicji Cyber Protection według harmonogramu

Na karcie **Harmonogram** można skonfigurować harmonogram automatycznych aktualizacji definicji Cyber Protection dla każdego z następujących komponentów:

- Ochrona antywirusowa
- Ocena luk w zabezpieczeniach
- Zarządzanie poprawkami

Aby zmienić ustawienie aktualizacji definicji, przejdź do sekcji **Ustawienia** > **Ochrona** > **Aktualizacja definicji ochrony** > **Harmonogram**.

Typ harmonogramu:

- **Codziennie** — określ dni tygodnia, w które mają być aktualizowane definicje.
  Rozpocznij o — wybierz, o której godzinie mają być zaktualizowane definicje.
- **Co godzinę** — podaj bardziej precyzyjny, godzinowy harmonogram aktualizacji.
  Uruchamiaj co — określ częstość przeprowadzania aktualizacji.
  Od ... **Do** — określ zakres czasu, w którym mają być dokonywane aktualizacje.

Aktualizowanie definicji Cyber Protection na żądanie

Aby zaktualizować definicje Cyber Protection określonego komputera na żądanie

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Wybierz komputery, na których chcesz zaktualizować definicje ochrony, i kliknij **Aktualizuj definicje**.

© Acronis International GmbH, 2003-2024

Pamięć podręczna

Lokalizacja danych w pamięci podręcznej:

- Na komputerach z systemem Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Na komputerach z systemem Linux: `/opt/acronis/var/atp-downloader/Cache`
- Na komputerach z systemem macOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Aby zmienić ustawienie pamięci podręcznej, przejdź do sekcji **Ustawienia** > **Ochrona** > **Aktualizacja definicji ochrony** > **Pamięć podręczna**.

W polu **Przestarzałe pliki aktualizacji i dane zarządzania poprawkami** określ, po jakim czasie dane mają zostać usunięte z pamięci podręcznej.

Maksymalny rozmiar pamięci podręcznej (GB) dla agentów:

- **Rola aktualizatora** — umożliwia określenie rozmiaru pamięci podręcznej na komputerach z rolą aktualizatora.
- **Inne role** — podaj rozmiar pamięci podręcznej na innych komputerach.

Uwaga
Cyber Protection zbiera próbki wykrytego złośliwego oprogramowania do dodatkowej analizy, abyśmy mogli ulepszać nasze oprogramowanie. Ustawienie to można w każdej chwili zmienić na karcie **Ochrona**, wyłączając przełącznik **Zbieraj i przesyłaj próbki złośliwego oprogramowania do CPOC**.

Usługi Cyber Protection instalowane w danym środowisku

Cyber Protection instaluje tylko niektóre z poniższych usług lub je wszystkie, w zależności od używanych opcji programu Cyber Protection.

Usługi instalowane w systemie Windows

Nazwa usługi	Przeznaczenie
Acronis Managed Machine Service	Udostępnia funkcje tworzenia kopii zapasowych, odzyskiwania, replikacji, przechowywania, weryfikacji
Acronis Scheduler2 Service	Wykonuje zaplanowane zadania w przypadku pewnych zdarzeń
Acronis Active Protection Service	Zapewnia ochronę przed oprogramowaniem wymuszającym okup

© Acronis International GmbH, 2003-2024

Acronis Cyber Protection Service	Zapewnia ochronę antywirusową

Usługi instalowane w systemie macOS

Nazwa i lokalizacja usługi	Przeznaczenie
`/Library/LaunchDaemons/com.acronis.aakore.plist`	Obsługuje komunikację między agentem a komponentami do zarządzania
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	Zapewnia wykrywanie złośliwego oprogramowania
`/Library/LaunchDaemons/com.acronis.mms.plist`	Udostępnia funkcje tworzenia kopii zapasowych i odzyskiwania
`/Library/LaunchDaemons/com.acronis.schedule.plist`	Wykonuje zaplanowane zadania

Zapisywanie pliku dziennika agenta

Dziennik agenta można zapisać w pliku .zip. Jeśli utworzenie kopii zapasowej nie powiedzie się z jakiegoś nieznanego powodu, plik ten pomoże personelowi odpowiedzialnemu za pomoc techniczną w zidentyfikowaniu problemu.

Domyślnie informacje zapisane w dzienniku są zoptymalizowane pod kątem ostatnich trzech dni, ale ten okres można zmienić.

Aby zebrać dzienniki agentów

1. Wykonaj jedną z następujących czynności:
   - W obszarze **Urządzenia** wybierz komputer, z którego chcesz zebrać dzienniki, a następnie kliknij **Działania**.
   - W sekcji **Ustawienia** > **Agenci** wybierz komputer, z którego chcesz zebrać dzienniki, a następnie kliknij **Szczegóły**.
2. [Opcjonalnie] Aby zmienić domyślny okres, z którego są uwzględniane informacje o systemie, kliknij strzałkę obok przycisku **Zbierz informacje o systemie**, a następnie wybierz okres.
3. Kliknij **Zbierz informacje o systemie**.
4. Jeśli przeglądarka wyświetli monit, określ, gdzie ma zostać zapisany plik.

Połączenie Open VPN site-to-site — dodatkowe informacje

Tworząc serwer odzyskiwania, konfiguruje się jego **Adres IP w sieci produkcyjnej** oraz jego **testowy adres IP**.

© Acronis International GmbH, 2003-2024

Po przeprowadzeniu przełączania awaryjnego (uruchomieniu maszyny wirtualnej w chmurze) i zalogowaniu się do maszyny wirtualnej w celu sprawdzenia adresu IP serwera pojawia się sekcja **Adres IP w sieci produkcyjnej**.

Po wykonaniu testowego przełączania awaryjnego komunikacja z serwerem testowym jest możliwa tylko wtedy, gdy się poda **Testowy adres IP**, który jest widoczny tylko w konfiguracji serwera odzyskiwania.

Aby uzyskać dostęp do serwera testowego z lokalizacji lokalnej, trzeba zastosować **Testowy adres IP**.

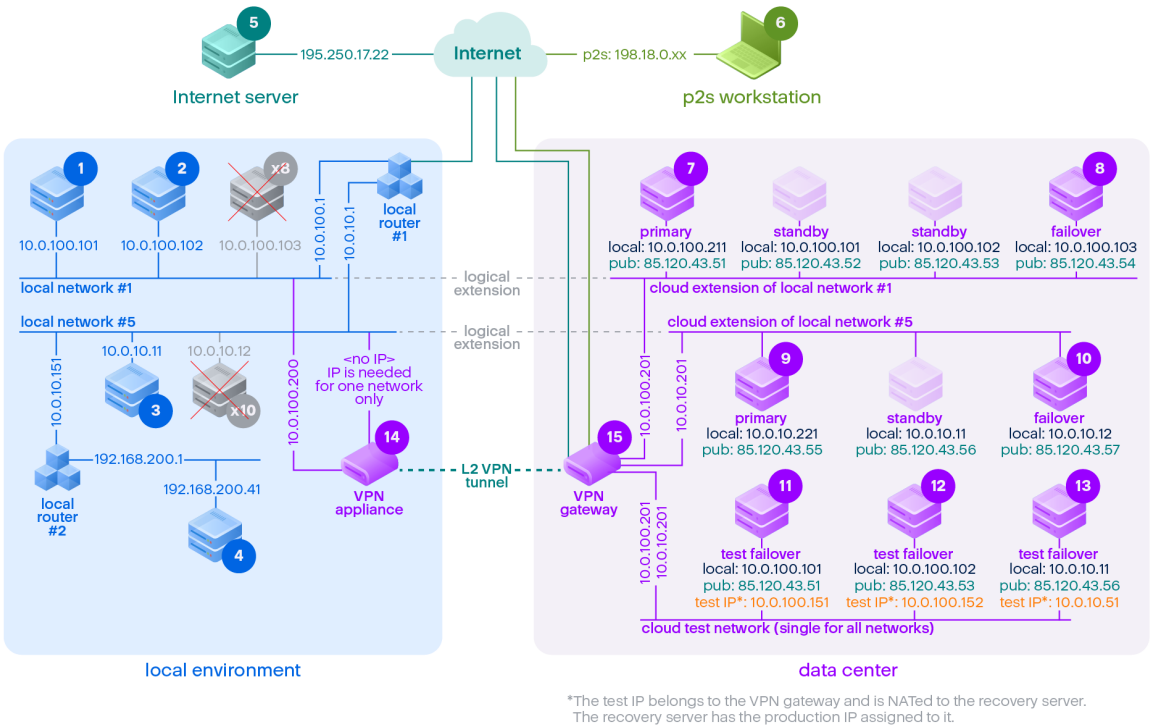
Uwaga
Konfiguracja sieci na serwerze zawsze zawiera **Adres IP w sieci produkcyjnej** (ponieważ serwer testowy odzwierciedla serwer produkcyjny). Jest tak, ponieważ testowy adres IP należy nie do serwera testowego, tylko do bramy VPN, i jest zmieniany na produkcyjny adres IP za pomocą translatora adresów sieciowych.

Poniższy diagram przedstawia przykładową konfigurację połączenia Open VPN site-to-site. Część serwerów znajdujących się w środowisku lokalnym jest odzyskiwanych w chmurze metodą przełączania awaryjnego (gdy infrastruktura sieci jest poprawna).

1. Klient włączył usługę Odzyskiwanie po awarii przez:
   a. skonfigurowanie urządzenia VPN (14) i podłączenie go do specjalnego chmurowego serwera VPN (15)
   b. objęcie wybranych serwerów lokalnych ochroną w ramach usługi Odzyskiwanie po awarii (1, 2, 3, x8 i x10)

      Niektóre serwery w lokalizacji lokalnej (np. 4) są podłączone do sieci, które nie są podłączone do urządzenia VPN. Takie serwery nie są chronione przy użyciu usługi Odzyskiwanie po awarii.
2. Część tych serwerów (podłączonych do różnych sieci) działa w lokalizacji lokalnej: (1, 2, 3 i 4)
3. Chronione serwery (1, 2 i 3) są poddawane testom w ramach testowego przełączania awaryjnego (11, 12 i 13)
4. Niektóre serwery w lokalizacji lokalnej są niedostępne (x8, x10). Po przełączeniu awaryjnym stają się one dostępne w chmurze (8 i 10)
5. Niektóre serwery podstawowe (7 i 9), podłączone do różnych sieci, są dostępne w środowisku chmurowym
6. (5) to serwer w Internecie z publicznym adresem IP
7. (6) to stacja robocza podłączona do chmury za pośrednictwem połączenia VPN point-to-site (p2s)

© Acronis International GmbH, 2003-2024



W tym przykładzie dostępna jest następująca konfiguracja połączenia (na przykład „ping”) od serwera w wierszu **Od:** do serwera w kolumnie **Do:**.

	Do:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Od:		lokalny	lokalny	lokalny	lokalny	Internet	p2s	podstawowe	przełączanie awaryjne	podstawowe	przełączanie awaryjne	testowe przełączanie awaryjne	testowe przełączanie awaryjne	testowe przełączanie awaryjne	urządzenie VPN	serwer VPN
1	lokalny		bezpośrednio	przez router lokalny 1	przez router lokalny 2	przez router lokalny 1 i Inter	nie	przez tunel: lokalny przez router lokalny 1	przez tunel: lokalny przez router lokalny 1	przez tunel: lokalny przez router lokalny 1	przez tunel: lokalny przez router lokalny 1	przez tunel: NAT (serwer VPN) przez router	przez tunel: NAT (serwer VPN) przez router	przez router lokalny 1 i tunel: NAT (serwer VP	bezpośrednio	nie

© Acronis International GmbH, 2003-2024

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						net		i Internet: publiczny	i Internet: publiczny	i Internet: publiczny	i Internet: publiczny	lokalny 1 i Internet: publiczny	lokalny 1 i Internet: publiczny	N) przez router lokalny 1 i Internet: publiczny		
2	lokalny	bezpośrednio		przez router lokalny 1	przez router lokalny 2	przez router lokalny 1 i Internet	nie	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	przez router lokalny 1 i tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	bezpośrednio	nie
3	lokalny	przez	przez		pr	pr	ni	przez	przez	przez	przez	przez	przez	prze	przez	nie

© Acronis International GmbH, 2003-2024

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		router lokalny 1	router lokalny 1		ze zrouterlokalny 2	ze zrouterlokalny 1 i Internet	e	tunel: lokalny przez router lokalny 1 i Internet: publiczny	tunel: lokalny przez router lokalny 1 i Internet: publiczny	tunel: lokalny przez router lokalny 1 i Internet: publiczny	tunel: lokalny przez router lokalny 1 i Internet: publiczny	tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	z router lokalny 1 i tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	router lokalny	
4	lokalny	przez router lokalny 2 i router 1	przez router lokalny 2 i router 1	przez routerlokalny 2		przez routerlokalny 2, router 1 i Interne	nie	przez router lokalny 2 i tunel: lokalny przez router lokalny 2,	przez router lokalny 2 i tunel: lokalny przez router lokalny 2,	przez router lokalny 2 i tunel: lokalny przez router lokalny 2,	przez router lokalny 2 i tunel: lokalny przez router lokalny 2,	przez tunel: NAT (serwer VPN) przez router lokalny 2, router 1 i Inter	przez tunel: NAT (serwer VPN) przez router lokalny 2, router 1 i Inter	przez tunel: NAT (serwer VPN) przez router lokalny 2, rout	przez router lokalny 2	nie

© Acronis International GmbH, 2003-2024

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						t		router lokalny 1 i Internet: publiczny	router lokalny 1 i Internet: publiczny	router lokalny 1 i Internet: publiczny	router lokalny 1 i Internet: publiczny	net: publiczny	net: publiczny	er 1 i Internet: publiczny		
5	Internet	nie	nie	nie	nie		n/d	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	nie	nie
6	p2s	nie	nie	nie	nie	przez Internet		przez VPN p2s (serwer VPN): lokalny przez Internet: publiczny	przez VPN p2s (serwer VPN): lokalny przez Internet: publiczny	przez VPN p2s (serwer VPN): lokalny przez Internet: publiczny	przez VPN p2s (serwer VPN): lokalny przez Internet: publiczny	przez VPN p2s — NAT (serwer VPN) przez Internet: publiczny	przez VPN p2s — NAT (serwer VPN) przez Internet: publiczny	przez VPN p2s — NAT (serwer VPN) przez Internet: publiczny	nie	nie
7	podstawowe	przez tunel	przez tunel	przez tunel i	przez tunel i	przez Internet	nie		bezpośrednio w chmurze: lokalny	przez tunel i router lokalny 1:	przez tunel i router lokalny 1:	przez serwer VPN: NAT	przez serwer VPN: NAT	przez tunel i router lokalny	nie	Tylko protokoły DHCP

© Acronis International GmbH, 2003-2024

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				router lokalny 1	router lokalny 1 oraz 2	(przez serwer VPN)				lokalny	lokalny			1: NAT		i DNS
8	przełączanie awaryjne	przez tunel	przez tunel	przez tunel i router lokalny 1	przez tunel i router lokalny 1 oraz 2	przez Internet (przez serwer VPN)	nie	bezpośrednio w chmurze: lokalny		przez tunel i router lokalny 1: lokalny	przez tunel i router lokalny 1: lokalny	przez serwer VPN: NAT	przez serwer VPN: NAT	przez tunel i router lokalny 1: NAT	nie	Tylko protokoły DHCP i DNS
9	podstawowe	przez tunel i router lokalny 1	przez tunel i router lokalny 1	przez tunel	przez tunel	przez Internet (przez serwer VPN)	nie	przez tunel i router lokalny 1: lokalny	przez tunel i router lokalny 1: lokalny		bezpośrednio w chmurze: lokalny	przez tunel i router lokalny 1: NAT	przez tunel i router lokalny 1: NAT	przez serwer VPN: NAT	nie	Tylko protokoły DHCP i DNS

© Acronis International GmbH, 2003-2024

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	przełączanie awaryjne	przez tunel i router lokalny 1	przez tunel i router lokalny 1	przez tunel	przez tunel	przez Internet (przez serwer VPN)	nie	przez tunel i router lokalny 1: lokalny	przez tunel i router lokalny 1: lokalny	bezpośrednio w chmurze: lokalny		przez tunel i router lokalny 1: NAT	przez tunel i router lokalny 1: NAT	przez serwer VPN: NAT	nie	Tylko protokoły DHCP i DNS
11	testuj przełączanie awaryjne	nie	nie	nie	nie	przez Internet (przez serwer VPN)	nie	nie	nie	nie	nie		bezpośrednio w chmurze: lokalny	przez serwer VPN: lokalny (routing)	nie	Tylko protokoły DHCP i DNS
12	testuj przełączanie awaryjne	nie	nie	nie	nie	przez Internet (przez serwer VP	nie	nie	nie	nie	nie	bezpośrednio w chmurze: lokalny		przez serwer VPN: lokalny (routing)	nie	Tylko protokoły DHCP i DNS

© Acronis International GmbH, 2003-2024

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						N)										
13	testuj przełączanie awaryjne	nie	nie	nie	nie	przez Internet (przez serwer VPN)	nie	nie	nie	nie	nie	przez serwer VPN: lokalny (routing)	przez serwer VPN: lokalny (routing)		nie	Tylko protokoły DHCP i DNS
14	urządzenie VPN	bezpośrednio	bezpośrednio	przez router lokalny 1	przez router lokalny 2	przez Internet (router lokalny 1)	nie	nie	nie	nie	nie	nie	nie	nie		nie
15	serwer VPN	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	

Zarządzanie licencjami dla lokalnych serwerów zarządzania

Szczegółowe informacje na temat aktywowania lokalnego serwera zarządzania lub przydzielania mu licencji można znaleźć w sekcji Licencjonowanie w podręczniku użytkownika rozwiązania Cyber Protect.

© Acronis International GmbH, 2003-2024

Praca z planami

Opis planów

Uwaga
Dostępność niektórych funkcji zależy od pozycji oferty włączonych w przypadku Twojego konta.

Plan to zestaw konfiguracji i reguł, które można zastosować do jednej lub kilku maszyn, aby osiągnąć różne cele, takie jak utworzenie kopii zapasowej maszyny, ochrona maszyny przed złośliwym oprogramowaniem, monitorowanie wydajności maszyny itp.

Plan składa się z modułów, które można włączać lub wyłączać. Każdy moduł zawiera ustawienia powiązane z konkretną funkcją.

Wszystkie utworzone przez Ciebie plany są wyświetlane na karcie **Zarządzanie**.

Plan	Opis
Plan ochrony	Chroni dane na maszynie. Plan ochrony składa się z następujących modułów: • Kopia zapasowa • "Wdrażanie funkcji odzyskiwania po awarii" (s. 786) • Ochrona przed wirusami i złośliwym oprogramowaniem • Endpoint Detection and Response (EDR) • Filtrowanie adresów URL • Windows Defender Antivirus • Microsoft Security Essentials • Ocena luk w zabezpieczeniach • Zarządzanie poprawkami • Mapa ochrony danych • Kontrola urządzeń • Advanced Data Loss Prevention Więcej informacji na temat planów ochrony można znaleźć w sekcji "Plany ochrony i moduły" (s. 221).
Plan zarządzania zdalnego	Włącza funkcje pulpitu zdalnego i pomocy na maszynach zarządzanych. Aby uzyskać więcej informacji, zobacz sekcję "Plany zarządzania zdalnego" (s. 1082).
Plan skryptów	Umożliwia wykonywanie skryptów na wielu maszynach, zaplanowane wykonywanie skryptów i konfigurowanie dodatkowych ustawień skryptów. Aby uzyskać więcej informacji, zobacz sekcję "Plany skryptów" (s. 412).
Plan monitorowania	Monitoruje wydajność, sprzęt, oprogramowanie, system i parametry zabezpieczeń zarządzanych maszyn. Aby uzyskać więcej informacji, zobacz sekcję "Plany monitorowania" (s. 1156).

© Acronis International GmbH, 2003-2024

Plan	Opis
Kopie zapasowe aplikacji w chmurze	Tworzy kopie zapasowe aplikacji działających w chmurze za pomocą agentów, które działają w chmurze, i używa chmury jako lokalizacji kopii zapasowych. Dodatkowe informacje można znaleźć w sekcji "Plany tworzenia kopii zapasowych aplikacji w chmurze" (s. 248).
Plan skanowania kopii zapasowych	Skanuje kopie zapasowe w poszukiwaniu złośliwego oprogramowania (w tym ransomware).
Replikacja maszyny wirtualnej	Skanuje kopie zapasowe w poszukiwaniu złośliwego oprogramowania (w tym ransomware). Więcej informacji można znaleźć w sekcji "Replikacja maszyn wirtualnych" (s. 729).
Sprawdzanie poprawności	Sprawdza poprawność kopii zapasowej i weryfikuje, czy można odzyskać dane z kopii zapasowej. Więcej informacji można znaleźć w sekcji "Sprawdzanie poprawności" (s. 234).
Czyszczenie	Usuwa nieaktualne kopie zapasowe zgodnie z regułami przechowywania. Plan ten jest stosowany tylko do agentów i maszyn, a nie do kopii zapasowych z chmury do chmury. Aby uzyskać więcej informacji, zobacz sekcję "Czyszczenie" (s. 242).
Konwertowanie na maszynę wirtualną	Ten plan jest stosowany tylko do kopii zapasowych na poziomie dysku. Sprawdza, czy kopia zapasowa obejmuje wolumin systemowy i zawiera wszystkie informacje potrzebne do uruchomienia systemu operacyjnego, tak aby powstała maszyna wirtualna mogła się samodzielnie uruchamiać. Aby uzyskać więcej informacji, zobacz sekcję "Konwersja na maszynę wirtualną" (s. 243).
Replikacja kopii zapasowej	Replikuje kopię zapasową do innej lokalizacji. Aby uzyskać więcej informacji, zobacz sekcję "Replikacja kopii zapasowej" (s. 230).

Plany wbudowane

Plany wbudowane to plany wstępnie skonfigurowane z niektórymi najczęściej używanymi lub zalecanymi ustawieniami. Plany wbudowane są od razu dostępne do wyboru. Nie można zmieniać planów wbudowanych, ale po zastosowaniu planu wbudowanego do maszyny można edytować ustawienia.

Wbudowane plany są dostępne dla następujących typów planów: plany ochrony, plany monitorowania i plany zarządzania zdalnego.

Wbudowane plany ochrony

Poniższa tabela zawiera więcej informacji na temat wbudowanych planów ochrony.

© Acronis International GmbH, 2003-2024

Moduły i ustawienia	Wbudowane plany ochrony		
	Niezbędna ochrona	**Rozszerzona ochrona**	**Pełna ochrona**
	Minimalne przestoje i utrata danych, łatwe odzyskiwanie z krótkim czasem RPO i łatwa konserwacja	**Drugi poziom ochrony: ciągłość działania, proaktywne niwelowanie zagrożeń bezpieczeństwa i zgodność**	**Trzeci poziom ochrony: ciągłość działania, niemal zerowy czas RTO, proaktywne niwelowanie zagrożeń bezpieczeństwa, zapobieganie wyciekom danych i zgodność**
Kopia zapasowa	Wł.	Wł.	Wł.
Elementy uwzględniane w kopii zapasowej Elementy uwzględniane w kopii zapasowej	Cały komputer	Cały komputer	Cały komputer
Ciągła ochrona danych	Wyłączone	Wyłączone	Włączone
Lokalizacja docelowa kopii zapasowej	Chmura	Chmura	Chmura
Harmonogram	Od poniedziałku do piątku o 12:00 Dodatkowo włączone opcje i warunki uruchomienia: • Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu • Wznów pracę z trybu uśpienia lub hibernacji, aby rozpocząć planowaną operację tworzenia kopii zapasowej	Od poniedziałku do piątku o 00:00 Dodatkowo włączone opcje i warunki uruchomienia: • Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu • Wznów pracę z trybu uśpienia lub hibernacji, aby rozpocząć planowaną operację tworzenia kopii zapasowej • Oszczędzanie baterii: Nie uruchamiaj przy zasilaniu z baterii • Nie uruchamiaj przy połączeniu taryfowym	Od poniedziałku do piątku o 00:00 Dodatkowo włączone opcje i warunki uruchomienia: • Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu • Wznów pracę z trybu uśpienia lub hibernacji, aby rozpocząć planowaną operację tworzenia kopii zapasowej • Oszczędzanie baterii: Nie uruchamiaj przy zasilaniu z baterii • Nie uruchamiaj przy połączeniu taryfowym

© Acronis International GmbH, 2003-2024

Moduły i ustawienia	Wbudowane plany ochrony		
	Niezbędna ochrona	**Rozszerzona ochrona**	**Pełna ochrona**
	Minimalne przestoje i utrata danych, łatwe odzyskiwanie z krótkim czasem RPO i łatwa konserwacja	**Drugi poziom ochrony: ciągłość działania, proaktywne niwelowanie zagrożeń bezpieczeństwa i zgodność**	**Trzeci poziom ochrony: ciągłość działania, niemal zerowy czas RTO, proaktywne niwelowanie zagrożeń bezpieczeństwa, zapobieganie wyciekom danych i zgodność**
	• Oszczędzanie baterii: Nie uruchamiaj przy zasilaniu z baterii • Nie uruchamiaj przy połączeniu taryfowym		
Schemat tworzenia kopii zapasowych	Zawsze przyrostowe	Zawsze przyrostowe	Zawsze przyrostowe
Okres przechowywania	Przechowuj wszystkie kopie zapasowe przez 90 dni	Przechowuj wszystkie kopie zapasowe przez 90 dni	Przechowuj wszystkie kopie zapasowe przez 90 dni
Opcje tworzenia kopii zapasowych	Opcje domyślne	Opcje domyślne plus: • Wydajność i okno na utworzenie kopii zapasowej (zestaw zielony): Priorytet procesora: Niski Szybkość danych wyjściowych: 50%	Opcje domyślne plus: • Wydajność i okno na utworzenie kopii zapasowej (zestaw zielony): Priorytet procesora: Niski Szybkość danych wyjściowych: 50%
EDR	Wył.	Wył.	Wł.
Ochrona przed wirusami i złośliwym oprogramowaniem	Wł.	Wł.	Wł.
Active Protection	Wł.	Wł.	Wł.

© Acronis International GmbH, 2003-2024

Moduły i ustawienia	Wbudowane plany ochrony		
	Niezbędna ochrona	**Rozszerzona ochrona**	**Pełna ochrona**
	Minimalne przestoje i utrata danych, łatwe odzyskiwanie z krótkim czasem RPO i łatwa konserwacja	**Drugi poziom ochrony: ciągłość działania, proaktywne niwelowanie zagrożeń bezpieczeństwa i zgodność**	**Trzeci poziom ochrony: ciągłość działania, niemal zerowy czas RTO, proaktywne niwelowanie zagrożeń bezpieczeństwa, zapobieganie wyciekom danych i zgodność**
Zaawansowana ochrona przed złośliwym oprogramowaniem	Wł.	Wł.	Wł.
Ochrona folderów sieciowych	Wł.	Wł.	Wł.
Ochrona po stronie serwera	Wył.	Wył.	Wył.
Ochrona własna	Wł.	Wł.	Wł.
Wykrywanie procesów cryptominingu	Wł.	Wł.	Wł.
Kwarantanna	Usuń pliki z kwarantanny po 30 dniach	Usuń pliki z kwarantanny po 30 dniach	Usuń pliki z kwarantanny po 30 dniach
Mechanizm zachowań	Kwarantanna	Kwarantanna	Kwarantanna
Ochrona przed exploitami	Powiadom i zatrzymaj proces	Powiadom i zatrzymaj proces	Powiadom i zatrzymaj proces
Ochrona w czasie rzeczywistym	Kwarantanna	Kwarantanna	Kwarantanna
Zaplanuj skanowanie	Szybkie skanowanie: Kwarantanna O 20:00 od niedzieli do soboty Pełne skanowanie: Kwarantanna O 21:00 w środy i piątki	Szybkie skanowanie: Kwarantanna O 20:00 od niedzieli do soboty Pełne skanowanie: Kwarantanna O 21:00 w środy i piątki Dodatkowo włączone	Szybkie skanowanie: Kwarantanna O 20:00 od niedzieli do soboty Pełne skanowanie: Kwarantanna O 21:00 w środy i piątki Dodatkowo włączone

© Acronis International GmbH, 2003-2024

Moduły i ustawienia	Wbudowane plany ochrony		
	Niezbędna ochrona	**Rozszerzona ochrona**	**Pełna ochrona**
	Minimalne przestoje i utrata danych, łatwe odzyskiwanie z krótkim czasem RPO i łatwa konserwacja	**Drugi poziom ochrony: ciągłość działania, proaktywne niwelowanie zagrożeń bezpieczeństwa i zgodność**	**Trzeci poziom ochrony: ciągłość działania, niemal zerowy czas RTO, proaktywne niwelowanie zagrożeń bezpieczeństwa, zapobieganie wyciekom danych i zgodność**
	Dodatkowo włączone opcje i warunki uruchomienia: Wznów pracę z trybu uśpienia lub hibernacji, aby rozpocząć planowaną operację tworzenia kopii zapasowej	opcje i warunki uruchomienia: Wznów pracę z trybu uśpienia lub hibernacji, aby rozpocząć planowaną operację tworzenia kopii zapasowej	opcje i warunki uruchomienia: Wznów pracę z trybu uśpienia lub hibernacji, aby rozpocząć planowaną operację tworzenia kopii zapasowej
Wykluczenia	Brak	Brak	Brak
Filtrowanie adresów URL	Wył.	Wł.	Wł.
Dostęp do złośliwych witryn internetowych	Blokuj	Blokuj	Blokuj
Kategorie do filtrowania	Opcje domyślne	Opcje domyślne	Opcje domyślne
Wykluczenia	Brak	Brak	Brak
Moduł Microsoft Defender Antivirus	Wył.	Wył.	Wył.
Zarządzanie zaporą	Wył.	Wł.	Wł.
Microsoft Security Essentials	Wył.	Wył.	Wył.
Ocena luk w zabezpieczeniach	Wł.	Wł.	Wł.

© Acronis International GmbH, 2003-2024

Moduły i ustawienia	Wbudowane plany ochrony		
	Niezbędna ochrona	**Rozszerzona ochrona**	**Pełna ochrona**
	Minimalne przestoje i utrata danych, łatwe odzyskiwanie z krótkim czasem RPO i łatwa konserwacja	**Drugi poziom ochrony: ciągłość działania, proaktywne niwelowanie zagrożeń bezpieczeństwa i zgodność**	**Trzeci poziom ochrony: ciągłość działania, niemal zerowy czas RTO, proaktywne niwelowanie zagrożeń bezpieczeństwa, zapobieganie wyciekom danych i zgodność**
Zakres oceny luk w zabezpieczeniach	Produkty firmy Microsoft, produkty innych firm przeznaczone do systemu Windows, produkty Apple, produkty innych firm przeznaczone do systemu macOS, pakiet Scan Linux	Produkty firmy Microsoft, produkty innych firm przeznaczone do systemu Windows, produkty Apple, produkty innych firm przeznaczone do systemu macOS, pakiet Scan Linux	Produkty firmy Microsoft, produkty innych firm przeznaczone do systemu Windows, produkty Apple, produkty innych firm przeznaczone do systemu macOS, pakiet Scan Linux
Harmonogram	O 11:00, tylko w środę i piątek	O 11:00, tylko w środę i piątek	O 11:00, tylko w środę i piątek
Zarządzanie poprawkami	Wł.	Wł.	Wł.
Produkty firmy Microsoft	Wszystkie aktualizacje	Wszystkie aktualizacje	Wszystkie aktualizacje
Produkty innych firm przeznaczone do systemu Windows	Wszystkie aktualizacje	Wszystkie aktualizacje	Wszystkie aktualizacje
Harmonogram	O 12:30, tylko w środę i piątek	O 12:30, tylko w środę i piątek	O 12:30, tylko w środę i piątek
Kopia zapasowa przed aktualizacją	Wł.	Wł.	Wł.
Mapa ochrony danych	Wył.	Wył.	Wł.
Reguły dotyczące rozszerzeń i wyjątków	–	–	Opcje domyślne (66 rozszerzeń do wykrycia)

© Acronis International GmbH, 2003-2024

Moduły i ustawienia	Wbudowane plany ochrony		
	Niezbędna ochrona	**Rozszerzona ochrona**	**Pełna ochrona**
	Minimalne przestoje i utrata danych, łatwe odzyskiwanie z krótkim czasem RPO i łatwa konserwacja	**Drugi poziom ochrony: ciągłość działania, proaktywne niwelowanie zagrożeń bezpieczeństwa i zgodność**	**Trzeci poziom ochrony: ciągłość działania, niemal zerowy czas RTO, proaktywne niwelowanie zagrożeń bezpieczeństwa, zapobieganie wyciekom danych i zgodność**
Harmonogram	–	–	O 15:40, od poniedziałku do piątku
Kontrola urządzeń	Wył.	Wył.	Wył.
Ustawienia dostępu	Zezwolenie: Wszystkie	Zezwolenie: Wszystkie	Zezwolenie: Wszystkie
Lista dozwolonych typów urządzeń	1 dozwolony (USD HID (mysz, klawiatura itp.)	1 dozwolony (USD HID (mysz, klawiatura itp.)	1 dozwolony (USD HID (mysz, klawiatura itp.)
Lista dozwolonych urządzeń USB	Pusty	Pusty	Pusty
Wykluczenie	Brak	Brak	Brak
Zapobieganie utracie danych	Wył.	Wył.	Wył.
Tryb	–	–	–
Ustawienia zaawansowane	–	–	–
Odzyskiwanie po awarii	Wył.	Wył.	Wył.

Dodatkowe informacje na temat planów ochrony można znaleźć w sekcji "Plany ochrony i moduły" (s. 221).

Wbudowane plany monitorowania

Poniższa tabela zawiera więcej informacji na temat wbudowanych planów monitorowania.

Nazwa	Opis	Włączone monitory
Zalecane w przypadku	Monitoruje kondycję i wydajność	W tym planie jest włączonych

© Acronis International GmbH, 2003-2024

Nazwa	Opis	Włączone monitory
systemu Windows	komputerów z systemem Windows	następujących 13 monitorów: • Status oprogramowania antywirusowego • Status funkcji uruchamiania automatycznego • Temperatura procesora • Użycie procesora • Miejsce na dysku • Szybkość transferu dysku • Niepowodzenia logowania • Status zapory • Temperatura procesora graficznego • Ostatnie ponowne uruchomienie systemu • Użycie pamięci • Wykorzystanie sieci • Status usługi Windows Update
Zalecane w przypadku systemu macOS	Monitoruje kondycję i wydajność komputerów z systemem macOS	W tym planie jest włączonych następujących 10 monitorów: • Status oprogramowania antywirusowego • Temperatura procesora • Użycie procesora • Miejsce na dysku • Szybkość transferu dysku • Status zapory • Temperatura procesora graficznego • Ostatnie ponowne uruchomienie systemu • Użycie pamięci • Wykorzystanie sieci
Zalecane w przypadku serwerów	Monitoruje kondycję i wydajność serwerów z systemem Windows	W tym planie jest włączonych następujących 20 monitorów: • Status oprogramowania antywirusowego • Temperatura procesora, 2 monitory: 26,7 stopnia, 10 min,

© Acronis International GmbH, 2003-2024

Nazwa	Opis	Włączone monitory
		ostrzeżenie 32,2 stopnia, 10 min, krytyczny • Użycie procesora, 3 monitory: Mniej niż 20%, 10 min, informacja Ponad 80%, 10 min, ostrzeżenie Ponad 90%, 10 min, krytyczny • Miejsce na dysku, 2 monitory: Mniej niż 20%, 30 min, ostrzeżenie Mniej niż 10%, 30 min, krytyczny • Szybkość transferu dysku • Nieudane logowania, 3 monitory: 5 prób, 1 godzina, informacja 10 prób, 1 godzina, ostrzeżenie 20 prób, 1 godzina, krytyczny • Status zapory • Zmiany sprzętowe • Zainstalowane oprogramowanie • Użycie pamięci, 3 monitory: Mniej niż 20%, 10 min, informacja Ponad 80%, 10 min, ostrzeżenie Ponad 90%, 10 min, krytyczny • Wykorzystanie sieci • Status usługi Windows Update

Dodatkowe informacje na temat planów monitorowania można znaleźć w sekcji "Plany monitorowania" (s. 1156).

Wbudowane plany zarządzania zdalnego

Poniższa tabela zawiera więcej informacji na temat wbudowanego planu zarządzania zdalnego.

Nazwa	Opis	Ustawienia
Podstawowy pulpit zdalny	Umożliwia korzystanie z funkcji pulpitu zdalnego i przesyłania plików	Protokoły połączenia **Zezwalaj na połączenia przez NEAR** : Włączono Ustawienia zabezpieczeń NEAR • **Zablokuj obciążenie, gdy użytkownik się**

© Acronis International GmbH, 2003-2024

Nazwa	Opis	Ustawienia
		rozłączy z sesją konsoli: Wyłączono • **Zezwól tylko jednemu użytkownikowi na połączenie przez NEAR lub przesyłanie plików w danym czasie**: Wyłączono • **Zezwól administratorowi obciążenia na połączenie z dowolną sesją**: Włączono • **Zezwól na tworzenie sesji systemowych**: Wyłączono • **Zezwól na synchronizację schowka**: Włączono **Zezwól na połączenia przez RDP** : Włączono **Zezwól na połączenia przez aplikację Udostępnianie ekranu firmy Apple**: Wyłączono Ustawienia zabezpieczeń • **Pokaż, czy obciążenie jest sterowane zdalnie**: Włączono • **Poproś użytkownika o zgodę na wykonanie zrzutów ekranu obciążenia**: Włączono Zarządzanie maszynami • **Przesyłanie plików**: Włączono • **Przesyłanie zrzutów ekranu**: Wyłączono Ustawienia wyświetlania • **Użyj funkcji powielania pulpitu w celu przechwycenia obrazu pulpitu**: Włączono • **Użyj funkcji przyspieszenia OpenCL**: Włączono • **Użyj funkcji kodowania sprzętowego H.264**: Włączono Przybornik **Pokaż ostatnio zalogowanych użytkowników**: Wyłączono

Aby uzyskać więcej informacji na temat planów zarządzania zdalnego, zobacz sekcję "Plany zarządzania zdalnego" (s. 1082).

Plany domyślne

Plan domyślny to plan, który będzie już zaznaczony na liście planów w polach wyboru planów. W danym czasie można mieć tylko jeden plan domyślny na dzierżawcę w przypadku każdego obsługiwanego typu planu. Planu domyślnego nie można usunąć, dopóki inny plan nie zostanie ustawiony jako domyślny.

© Acronis International GmbH, 2003-2024

Plany domyślne są obsługiwane w przypadku następujących typów planów: plany ochrony, plany monitorowania i plany zarządzania zdalnego.

Ustawianie planów jako domyślnych

Jeden plan spośród obsługiwanych typów planów (plan ochrony, plan monitorowania lub plan zarządzania zdalnego) można ustawić jako domyślny.

Uwaga
Ta funkcja nie jest dostępna dla użytkowników, którym przypisano rolę administratora Tylko do odczytu dla usługi Protection.

Plany ochrony

Wymagania wstępne

Dla dzierżawcy utworzono co najmniej jeden plan ochrony. Aby uzyskać więcej informacji, zobacz sekcję "Tworzenie planu ochrony" (s. 222).

Aby ustawić plan ochrony jako domyślny

1. Na ekranie **Plany ochrony** znajdź plan, który chcesz ustawić jako domyślny, a następnie go kliknij.
2. Kliknij **Ustaw jako domyślne**.
3. W oknie potwierdzenia kliknij **Ustaw**.
   Na ekranie **Plany ochrony** obok nazwy planu będzie widoczny znacznik **Domyślne**.

Plany zarządzania zdalnego

Wymagania wstępne

- Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.
- Dla dzierżawy utworzono co najmniej jeden plan zarządzania zdalnego. Aby uzyskać więcej informacji, zobacz sekcję "Tworzenie planu zarządzania zdalnego" (s. 1083).

Aby ustawić plan zarządzania zdalnego jako domyślny

1. Na ekranie **Plany zarządzania zdalnego** znajdź plan, który chcesz ustawić jako domyślny.
2. W tym samym wierszu kliknij ikonę **Więcej czynności**.
3. Kliknij **Ustaw jako domyślne**.
4. W oknie potwierdzenia kliknij **Ustaw**.
   Na ekranie **Plany zdalnego zarządzania** obok nazwy planu jest widoczny znacznik **Domyślne**.

Plany monitorowania

© Acronis International GmbH, 2003-2024

Wymagania wstępne

- Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.
- Dla dzierżawcy utworzono co najmniej jeden plan monitorowania. Aby uzyskać więcej informacji, zobacz sekcję "Tworzenie planu monitorowania" (s. 1157).

Aby ustawić plan monitorowania jako zdalny

1. Na ekranie **Plany monitorowania** znajdź plan, który chcesz ustawić jako domyślny.
2. W tym samym wierszu kliknij ikonę **Więcej czynności**.
3. Kliknij **Dodaj do ulubionych**.
4. W oknie potwierdzenia kliknij **Ustaw**.
   Na ekranie **Plany monitorowania** obok nazwy planu będzie widoczny znacznik **Domyślne**.

Ulubione plany

Ulubione plany są wyświetlane na początku listy planów. Jeśli ustawisz plan jako ulubiony, masz pewność, że będzie on dobrze widoczny i będzie można go łatwo znaleźć, nawet jeśli organizacja ma długą listę zawierającą wiele planów.

Ulubione plany są obsługiwane w przypadku następujących typów planów: plany ochrony, plany monitorowania i plany zarządzania zdalnego.

Ustawianie planów jako ulubionych

Możesz skonfigurować nawet 10 ulubionych planów w przypadku każdego obsługiwanego typu planu (planu ochrony, planu monitorowania lub planu zarządzania zdalnego) na dzierżawcę.

Uwaga
Ta funkcja nie jest dostępna dla użytkowników, którym przypisano rolę administratora Tylko do odczytu dla usługi Protection.

Plany ochrony

Wymagania wstępne

Dla dzierżawcy utworzono co najmniej jeden plan ochrony. Aby uzyskać więcej informacji, zobacz sekcję "Tworzenie planu ochrony" (s. 222).

Aby ustawić plan ochrony jako ulubiony

1. Na ekranie **Plany ochrony** kliknij plan, który chcesz ustawić jako ulubiony.
2. Kliknij **Ustaw jako ulubione**.
   Na ekranie **Plany ochrony** obok nazwy planu będzie widoczna ikona gwiazdki.

Plany zarządzania zdalnego

© Acronis International GmbH, 2003-2024

Wymagania wstępne

- Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.
- Dla dzierżawy utworzono co najmniej jeden plan zarządzania zdalnego. Aby uzyskać więcej informacji, zobacz sekcję "Tworzenie planu monitorowania" (s. 1157).

Aby ustawić plan zarządzania zdalnego jako ulubiony

1. Na ekranie **Plany zarządzania zdalnego** znajdź plan, który chcesz ustawić jako ulubiony.
2. W wierszu planu kliknij ikonę **Więcej czynności**.
3. Kliknij **Dodaj do ulubionych**.
   Na ekranie **Plany zarządzania zdalnego** obok nazwy będzie widoczna ikona gwiazdki.

Plany monitorowania

Wymagania wstępne

- Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.
- Dla dzierżawy utworzono co najmniej jeden plan zarządzania. Aby uzyskać więcej informacji, zobacz sekcję "Tworzenie planu monitorowania" (s. 1157).

Aby ustawić plan monitorowania jako ulubiony

1. Na ekranie **Plany monitorowania** znajdź plan, który chcesz ustawić jako ulubiony.
2. W wierszu planu kliknij ikonę **Więcej czynności**.
3. Kliknij **Dodaj do ulubionych**.
   Na ekranie **Plany monitorowania** obok nazwy planu będzie widoczna ikona gwiazdki.

Usuwanie planów z ulubionych

Możesz usuwać plany ochrony, plany monitorowania i plany zarządzania zdalnego z listy ulubionych.

Uwaga
Ta funkcja nie jest dostępna dla użytkowników, którym przypisano rolę administratora Tylko do odczytu dla usługi Protection.

Plany ochrony

Wymagania wstępne

Dla Twojego dzierżawcy ustawiono jako ulubiony co najmniej jeden plan ochrony.

Aby usunąć plan ochrony z ulubionych

1. Na ekranie **Plany ochrony** kliknij plan, który chcesz usunąć z ulubionych.
2. Kliknij **Usuń z ulubionych**.

Plany zarządzania zdalnego

© Acronis International GmbH, 2003-2024

Wymagania wstępne

- Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.
- Dla Twojego dzierżawcy ustawiono jako ulubiony co najmniej jeden plan zarządzania zdalnego.

Aby usunąć plan zdalnego zarządzania z ulubionych

1. Na ekranie **Plany zarządzania zdalnego** kliknij plan, który chcesz usunąć z ulubionych.
2. W wierszu planu kliknij ikonę **Więcej czynności**.
3. Kliknij **Usuń z ulubionych**.

Plany monitorowania

Wymagania wstępne

- Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.
- Dla Twojego dzierżawcy ustawiono jako ulubiony co najmniej jeden plan monitorowania.

Aby usunąć plan monitorowania z ulubionych

1. Na ekranie **Plany monitorowania** znajdź plan, który chcesz usunąć z ulubionych.
2. W wierszu planu kliknij ikonę **Więcej czynności**.
3. Kliknij **Usuń z ulubionych**.

Plany ochrony i moduły

Aby chronić swoje dane, należy utworzyć plany ochrony, a następnie zastosować je do swoich maszyn.

Plan ochrony obejmuje różne moduły ochrony. Włącz potrzebne moduły i skonfiguruj ich ustawienia, aby utworzyć plany ochrony zaspokajające Twoje potrzeby.

Dostępne są następujące moduły:

- Kopia zapasowa. Umożliwia tworzenie kopii zapasowych źródeł danych na dysku lokalnym lub w chmurze.
- "Wdrażanie funkcji odzyskiwania po awarii" (s. 786). Umożliwia uruchamianie dokładnych kopii komputerów w lokalizacji w chmurze i przenoszenie obciążeń z uszkodzonych pierwotnych komputerów na serwery odzyskiwania w chmurze.
- Ochrona przed wirusami i złośliwym oprogramowaniem. Umożliwia sprawdzanie obciążeń przy użyciu wbudowanego rozwiązania do ochrony przed złośliwym oprogramowaniem.
- Endpoint Detection and Response (EDR). Wykrywa podejrzane działania na obciążeniu, w tym dotąd niezauważone ataki, i generuje incydenty, aby pomóc w ustaleniach, jak doszło do ataku i jak zapobiec jego ponownemu wystąpieniu.

© Acronis International GmbH, 2003-2024

- Filtrowanie adresów URL. Umożliwia chronienie komputerów przed zagrożeniami z Internetu przez blokowanie dostępu do złośliwych adresów URL i dostępnych do pobrania treści.
- Program antywirusowy Windows Defender. Umożliwia zarządzanie ustawieniami programu antywirusowego Windows Defender w celu zapewnienia ochrony danego środowiska.
- Microsoft Security Essentials. Umożliwia zarządzanie ustawieniami programu Microsoft Security Essentials w celu zapewnienia ochrony danego środowiska.
- Ocena luk w zabezpieczeniach. Sprawdza zainstalowane na komputerach systemy Windows, Linux i macOS, produkty innych firm dla systemu firmy Microsoft oraz produkty innych firm dla systemu macOS pod kątem występowania luk w zabezpieczeniach, a następnie powiadamia użytkownika o ich ewentualnym występowaniu.
- Zarządzanie poprawkami. Umożliwia instalowanie na komputerach poprawek i aktualizacji systemów Windows, Linux i macOS, produktów innych firm dla systemu firmy Microsoft oraz produktów innych firm dla systemu macOS w celu wyeliminowania wykrytych luk w zabezpieczeniach.
- Mapa ochrony danych. Umożliwia wykrywanie danych w celu monitorowania statusu ochrony ważnych plików.
- Kontrola urządzeń. Umożliwia wskazanie urządzeń, których użytkownicy mogą używać na swoich komputerach lub których używania zabroniono.
- Advanced Data Loss Prevention. Dzięki zasadom przepływów danych moduł ten zapobiega wyciekowi poufnych danych za pośrednictwem urządzeń peryferyjnych (takich jak drukarki czy magazyny wymienne) lub przez przesyłanie danych przez sieć wewnętrzną bądź zewnętrzną.

Tworzenie planu ochrony

Plan ochrony można utworzyć w jeden z następujących sposobów:

- Na karcie **Urządzenia**. Wybierz obciążenia, które mają być chronione, a następnie utwórz dla nich plan ochrony.
- Na karcie **Zarządzanie** > **Plany ochrony**. Utwórz plan ochrony, a następnie wybierz maszyny, do których ma on zostać zastosowany.

Podczas tworzenia planu ochrony widoczne są tylko te moduły, których można użyć w przypadku danego typu obciążenia.

Plan ochrony można zastosować do więcej niż jednej maszyny. Można też zastosować kilka planów ochrony do jednej maszyny. Dodatkowe informacje na temat możliwych konfliktów można znaleźć w sekcji "Usuwanie konfliktów między planami" (s. 228).

Aby utworzyć plan ochrony

Urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz obciążenia, które chcesz chronić, i kliknij **Chroń**.
3. [W przypadku już zastosowanych planów] Kliknij **Dodaj plan**.

© Acronis International GmbH, 2003-2024

4. Kliknij **Utwórz plan** > **Ochrona**.

   Otworzy się panel planu ochrony.
5. [Opcjonalnie] Aby zmienić nazwę planu ochrony, kliknij ikonę ołówka, a następnie wprowadź nową nazwę.
6. [Opcjonalnie] Aby włączyć lub wyłączyć moduł w planie, przełącz przełącznik widoczny obok nazwy modułu.
7. [Opcjonalnie] W celu skonfigurowania modułu kliknij go, aby go rozwinąć, a następnie zmień ustawienia stosownie do potrzeb.
8. Gdy skończysz, kliknij **Utwórz**.

Uwaga
Aby utworzyć plan ochrony z szyfrowaniem, określ hasło szyfrowania. Dodatkowe informacje można znaleźć w sekcji "Szyfrowanie" (s. 474).

Zarządzanie > Plany ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Kliknij **Utwórz plan**.

   Zostanie otwarty szablon planu ochrony.
3. [Opcjonalnie] Aby zmienić nazwę planu ochrony, kliknij ikonę ołówka, a następnie wprowadź nową nazwę.
4. [Opcjonalnie] Aby włączyć lub wyłączyć moduł w planie, przełącz przełącznik widoczny obok nazwy modułu.
5. [Opcjonalnie] W celu skonfigurowania modułu kliknij go, aby go rozwinąć, a następnie zmień ustawienia stosownie do potrzeb.
6. [Opcjonalnie] Aby wybrać obciążenia, do których ma zostać zastosowany plan, kliknij **Dodaj urządzenia**.

   Uwaga
   Możesz jednak utworzyć plan i nie zastosować go do żadnej maszyny. Maszyny można dodać później, edytując w tym celu plan. Dodatkowe informacje na temat dodawania maszyny do planu można znaleźć w sekcji "Stosowanie planu ochrony do obciążenia" (s. 225).
7. Gdy skończysz, kliknij **Utwórz**.

   Uwaga
   Aby utworzyć plan ochrony z szyfrowaniem, określ hasło szyfrowania. Dodatkowe informacje można znaleźć w sekcji "Szyfrowanie" (s. 474).

Aby uruchomić moduł (taki jak **Kopia zapasowa**, **Ochrona przed wirusami i złośliwym oprogramowaniem**, **Ocena luk w zabezpieczeniach**, **Zarządzanie poprawkami** lub **Mapa ochrony danych**) na żądanie, kliknij **Uruchom teraz**.

Obejrzyj instruktaż wideo Tworzenie pierwszego planu ochrony.

© Acronis International GmbH, 2003-2024

Więcej informacji na temat modułu Odzyskiwanie po awarii można znaleźć w sekcji "Tworzenie planu ochrony na potrzeby odzyskiwania po awarii" (s. 793).

Więcej informacji na temat modułu Kontrola urządzeń można znaleźć w sekcji "Korzystanie z modułu kontroli urządzeń" (s. 360).

Czynności dotyczące planów ochrony

Po utworzeniu planu ochrony można wykonywać następujące dotyczące go czynności:

- Zastosować plan do obciążenia lub grupy urządzeń.
- Zmienianie nazwy planu.
- Edytować plan.
  Włączyć lub wyłączyć moduły w planie oraz zmienić ich ustawienia.
- Włączyć lub wyłączyć plan.
  Wyłączony plan nie będzie wykonywany na obciążeniach, do których go zastosowano.
  Ta czynność jest wygodna dla administratorów, którzy zamierzają później chronić dane obciążenie przy użyciu tego samego planu. Ponieważ plan nie zostaje odwołany z obciążenia, można szybko wznowić ochronę przez ponowne włączenie planu.
- Odwołać plan z obciążenia.
  Odwołany plan nie będzie już zastosowany do danego obciążenia.
  Ta czynność jest wygodna dla administratorów, którzy nie muszą szybko włączyć ochrony tego obciążenia przy użyciu tego samego planu. Aby przywrócić ochronę zapewnianą przez odwołany plan, trzeba znać jego nazwę, a następnie wybrać go z listy dostępnych planów i ponownie zastosować do odpowiedniego obciążenia.
- Zatrzymaj plan.
  Ta czynność spowoduje zatrzymanie wszystkich wykonywanych operacji tworzenia kopii zapasowej na wszystkich obciążeniach, do których zastosowano plan. Operacje tworzenia kopii zapasowych zostaną wznowione zgodnie z harmonogramem planu.
  Ta czynność nie wpływa na skanowanie antywirusowe i będzie ono kontynuowane zgodnie ze skonfigurowanym harmonogramem.
- Sklonować plan.
  Można utworzyć dokładną kopię już istniejącego planu. Nowy plan nie będzie przypisany do żadnego obciążenia.
- Wyeksportować lub zaimportować plan.
  Plan można wyeksportować jako plik JSON, który później można zaimportować z powrotem. Dzięki temu nie trzeba ręcznie tworzyć nowego planu i konfigurować jego ustawień.

  Uwaga
  Zaimportować można tylko plany ochrony utworzone w usłudze Cyber Protection 9.0 (wydanej w marcu 2020 r.) lub nowszej. Plany utworzone w starszych wersjach produktu nie są zgodne z programem Cyber Protection w wersji 9.0 lub nowszej.

© Acronis International GmbH, 2003-2024

- Sprawdzić szczegóły planu.
- Sprawdzić działania i alerty związane z planem.
- Usuwanie planu.

Stosowanie planu ochrony do obciążenia

Aby chronić obciążenie, należy zastosować do niego plan ochrony.

Plan można zastosować z poziomu karty **Urządzenia** oraz karty **Zarządzanie** > **Plany ochrony**.

Urządzenia

1. Wybierz obciążenia, które chcesz chronić.
2. Kliknij **Chroń**.
3. [Jeśli do wybranych obciążeń już zastosowano inny plan ochrony] Kliknij **Dodaj plan**.
4. Zostanie wyświetlona lista dostępnych planów ochrony.
5. Wybierz plan ochrony, który chcesz zastosować, i kliknij **Zastosuj**.

Zarządzanie > Plany ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Wybierz plan ochrony, który chcesz zastosować.
3. Kliknij **Edytuj**.
4. Kliknij **Zarządzaj urządzeniami**.
5. W oknie **Urządzenia** kliknij **Dodaj**.
6. Wybierz obciążenia, do których chcesz zastosować plan, a następnie kliknij **Dodaj**.
7. W oknie **Urządzenia** kliknij **Gotowe**.
8. W panelu planu ochrony kliknij **Zapisz**.

Aby się dowiedzieć, jak zastosować plan ochrony do grupy urządzeń, zobacz sekcję "Stosowanie planu do grupy" (s. 358).

Edytowanie planu ochrony

W ramach edycji planu można włączać i wyłączać znajdujące się w nim moduły oraz zmieniać ich ustawienia.

Plan ochrony można edytować z uwzględnieniem wszystkich obciążeń, do których jest on stosowany, lub tylko wybranych obciążeń.

Plan można edytować na karcie **Urządzenia** oraz karcie **Zarządzanie** > **Plany ochrony**.

Urządzenia

© Acronis International GmbH, 2003-2024

1. Wybierz obciążenia, do których zastosowano plan.
2. Kliknij **Chroń**.
3. Wybierz plan ochrony, który chcesz edytować.
4. Kliknij ikonę wielokropka (...) widoczną obok nazwy planu, a następnie kliknij **Edytuj**.
5. Kliknij moduł, który chcesz edytować, a następnie skonfiguruj jego ustawienia stosownie do potrzeb.
6. Kliknij **Zapisz**.
7. [Jeśli wybrano tylko niektóre maszyny, do których zastosowano plan] Wybierz zakres edycji:
   - Aby edytować plan ochrony z uwzględnieniem wszystkich obciążeń, do których go zastosowano, kliknij **Zastosuj zmiany do tego planu ochrony (będzie to mieć wpływ na inne urządzenia)**.
   - Aby zmienić plan tylko w odniesieniu do wybranych obciążeń, kliknij **Utwórz nowy plan ochrony tylko dla wybranych urządzeń**.

     W wyniku tych działań istniejący plan zostanie odwołany z wybranych obciążeń. Zostanie utworzony nowy plan ochrony ze skonfigurowanymi przez Ciebie ustawieniami i zastosowany do tych obciążeń.

Zarządzanie > Plany ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Wybierz plan ochrony, który chcesz edytować.
3. Kliknij **Edytuj**.
4. Kliknij moduły, które chcesz edytować, a następnie skonfiguruj ich ustawienia stosownie do potrzeb.
5. Kliknij **Zapisz**.

Uwaga
Edycja planu na karcie **Zarządzanie** > **Plany ochrony** będzie miała wpływ na wszystkie maszyny, do których zastosowano plan.

Odwoływanie planu ochrony

Odwołanie planu polega na usunięciu go z odpowiedniego obciążenia. Pozostałe obciążenia, do których został zastosowany plan, będą nadal chronione.

Plan można odwołać z poziomu karty **Urządzenia** oraz karty **Zarządzanie** > **Plany ochrony**.

Urządzenia

1. Wybierz obciążenia, z których chcesz odwołać plan.
2. Kliknij **Chroń**.
3. Wybierz plan ochrony, który chcesz odwołać.
4. Kliknij ikonę wielokropka (...) widoczną obok nazwy planu, a następnie kliknij **Odwołaj**.

© Acronis International GmbH, 2003-2024

Zarządzanie > Plany ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Wybierz plan ochrony, który chcesz odwołać.
3. Kliknij **Edytuj**.
4. Kliknij **Zarządzaj urządzeniami**.
5. W oknie **Urządzenia** wybierz obciążenia, z których chcesz odwołać plan.
6. Kliknij **Usuń**.
7. W oknie **Urządzenia** kliknij **Gotowe**.
8. W szablonie planu ochrony kliknij **Zapisz**.

Włączanie lub wyłączanie planu ochrony

Włączony plan jest aktywny i wykonywany na obciążeniach, do których został on zastosowany. Wyłączony plan jest nieaktywny — pozostaje zastosowany do obciążeń, ale nie jest na nich wykonywany.

Włączenie lub wyłączenie planu ochrony na karcie **Urządzenia** ma wpływ tylko na wybrane obciążenia.

Włączenie lub wyłączenie planu ochrony na karcie **Zarządzanie** > **Plany ochrony** ma wpływ na wszystkie obciążenia, do których ten plan został zastosowany. Ponadto można włączać lub wyłączać wiele planów ochrony.

Urządzenia

1. Wybierz obciążenie, którego plan chcesz wyłączyć.
2. Kliknij **Chroń**.
3. Wybierz plan ochrony, który chcesz wyłączyć.
4. Kliknij ikonę wielokropka (...) widoczną obok nazwy planu, a następnie kliknij odpowiednio **Włącz** lub **Wyłącz**.

Zarządzanie > Plany ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Wybierz co najmniej jeden plan ochrony, który chcesz włączyć lub wyłączyć.
3. Kliknij **Edytuj**.
4. Kliknij odpowiednio **Włącz** lub **Wyłącz**.

Uwaga
Ta czynność nie ma wpływu na plany ochrony, które już są w stanie docelowym. Jeśli na przykład wybór obejmuje zarówno włączone, jak i wyłączone plany, a użytkownik kliknie przycisk **Włącz**, wszystkie wybrane plany będą włączone.

© Acronis International GmbH, 2003-2024

Usuwanie planu ochrony

Usunięcie planu powoduje odwołanie go ze wszystkich obciążeń i usunięcie z konsoli Cyber Protect.

Plan można usunąć z poziomu karty **Urządzenia** oraz karty **Zarządzanie** > **Plany ochrony**.

Urządzenia

1. Wybierz dowolne obciążenie, do którego jest stosowany plan ochrony przeznaczony do usunięcia.
2. Kliknij **Chroń**.
3. Wybierz plan ochrony, który chcesz usunąć.
4. Kliknij ikonę wielokropka (...) widoczną obok nazwy planu, a następnie kliknij **Usuń**.

Zarządzanie > Plany ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Wybierz plan ochrony, który chcesz usunąć.
3. Kliknij **Usuń**.
4. Potwierdź wybór przez zaznaczenie pola wyboru **Potwierdzam usunięcie planu**, a następnie kliknij **Usuń**.

Usuwanie konfliktów między planami

Można zastosować kilka planów ochrony do jednego obciążenia. Na przykład można zastosować plan ochrony, w którym włączono i skonfigurowano tylko moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**, oraz plan ochrony, w którym włączono i skonfigurowano tylko moduł **Kopia zapasowa**.

Można łączyć plany ochrony, w których włączono różne moduły. Można też łączyć różne plany ochrony, w których włączono tylko moduł **Kopia zapasowa**. Jeśli jednak jakiś inny moduł zostanie włączony w więcej niż jednym planie, spowoduje to konflikt. Aby zastosować plan, trzeba będzie najpierw ten konflikt rozwiązać.

Konflikt między nowym a wcześniejszym planem

Jeśli nowy plan powoduje konflikt z jakimś wcześniejszym planem, konflikt ten można rozwiązać w jeden z następujących sposobów:

- Utworzyć nowy plan, zastosować go, a następnie wyłączyć wcześniejszy plan, który jest w konflikcie z nowym.
- Utworzyć nowy plan, a następnie go wyłączyć.

© Acronis International GmbH, 2003-2024

Konflikt między planem indywidualnym a planem grupy

Jeśli indywidualny plan ochrony powoduje konflikt z planem grupy zastosowanym do grupy urządzeń, konflikt ten można rozwiązać w jeden z następujących sposobów:

- Usunąć obciążenie z grupy urządzeń, a następnie zastosować do niego indywidualny plan ochrony.
- Edytować dany plan grupy lub zastosować nowy plan grupy do grupy urządzeń.

Problem z licencją

Moduł uwzględniony w planie ochrony może wymagać przypisania określonego limitu usługi do chronionego obciążenia. Jeśli przypisany limit usługi nie jest odpowiedni, nie będzie można uruchomić, zaktualizować ani zastosować planu ochrony, w którym włączono dany moduł.

Aby rozwiązać problem z licencją, wykonaj jedną z następujących czynności:

- Wyłącz moduł, który nie jest obsługiwany w ramach aktualnie przypisanego limitu usługi, i dalej korzystaj z planu ochrony.
- Ręcznie zmień przypisany limit usługi. Informacje o tym, jak to zrobić, można znaleźć w sekcji "Zmienianie limitów usług komputerów" (s. 193).

Indywidualne plany ochrony do hostingu integracji panelu kontrolnego

Po włączeniu hostingu integracji panelu kontrolnego na serwerach hostingu witryn internetowych, które używają rozwiązań DirectAdmin, cPanel lub Plesk, usługa Cyber Protection automatycznie tworzy indywidualny plan ochrony dla każdego obciążenia w ramach konta użytkownika. Taki plan ochrony jest powiązany z konkretnym obciążeniem, które zainicjowało tworzenie planu ochrony, i nie może być odwołany ani przypisany do innych obciążeń.

Aby przestać używać indywidualnego planu ochrony, możesz usunąć go z konsoli Cyber Protect.

Indywidualne plany ochrony można zidentyfikować dzięki znakowi obok ich nazwy.

Jeśli chcesz, aby plan ochrony chronił wiele serwerów hostingowych, które korzystają z integracji panelu kontrolnego hostingu, możesz utworzyć zwykły plan ochrony w konsoli Cyber Protect i przypisać do niego te obciążenia. Jednak wszelkie modyfikacje planu ochrony, który jest współdzielony przez wiele paneli kontrolnych hostingu, mogą być dokonywane wyłącznie w konsoli Cyber Protect, a nie z poziomu integracji.

© Acronis International GmbH, 2003-2024

Plany ochrony danych poza hostem

Uwaga
Ta funkcja jest dostępna w ramach dzierżawców-klientów, dla których włączono limit **Zaawansowane kopie zapasowe — serwery** lub **Zaawansowane kopie zapasowe — NAS** w ramach pakietu Advanced Backup.

Replikacja, sprawdzanie poprawności i czyszczenie są zwykle wykonywane przez agenta ochrony, który tworzy kopię zapasową. Powoduje to dodatkowe obciążenie komputera, na którym działa agent, nawet po zakończeniu procesu tworzenia kopii zapasowej. Aby odciążyć ten komputer, można utworzyć plany ochrony danych poza hostem — to znaczy osobne plany replikacji, sprawdzania poprawności, czyszczenia i konwersji na maszynę wirtualną.

Dzięki planom ochrony danych poza hostem możesz wykonywać następujące czynności:

- Wybierać różnych agentów do operacji tworzenia kopii zapasowych i ochrony danych poza hostem
- Planować wykonywanie operacji przetwarzania danych poza hostem w czasie poza godzinami szczytu, aby zminimalizować stopień wykorzystania przepustowości sieci
- Planować wykonywanie operacji przetwarzania danych poza hostem w czasie poza godzinami pracy, jeśli nie chcesz instalować osobnego agenta na potrzeby przetwarzania danych poza hostem

Uwaga
Plany przetwarzania danych poza hostem są wykonywane zgodnie z ustawieniami czasu (w tym strefy czasowej) komputera, na którym jest zainstalowany agent ochrony. W przypadku urządzenia wirtualnego (na przykład agenta dla VMware lub agenta dla Scale Computing HC3) strefę czasową można skonfigurować w graficznym interfejsie użytkownika agenta.

Replikacja kopii zapasowej

Uwaga
Ta funkcja jest dostępna w ramach dzierżawców-klientów, dla których włączono limit **Zaawansowane kopie zapasowe — serwery** lub **Zaawansowane kopie zapasowe — NAS** w ramach pakietu Advanced Backup.

Replikacja kopii zapasowej polega na skopiowaniu kopii zapasowej do innej lokalizacji. Ponieważ jest to operacja przetwarzania danych poza hostem, jest ona skonfigurowana w planie replikacji kopii zapasowych.

Replikacja kopii zapasowych może też stanowić część planu ochrony. Dodatkowe informacje na temat tej opcji można znaleźć w sekcji "Replikacja" (s. 472).

© Acronis International GmbH, 2003-2024

Tworzenie planu replikacji kopii zapasowej

Aby zreplikować kopie zapasowe w ramach operacji przetwarzania danych poza hostem, należy utworzyć plan replikacji kopii zapasowych.

Aby utworzyć plan replikacji kopii zapasowych

1. W konsoli Cyber Protect kliknij **Zarządzanie** > **Replikacja kopii zapasowej**.
2. Kliknij **Utwórz plan**.
3. W polu **Agent** wybierz agenta, który wykona replikację.
   Możesz wybrać dowolnego agenta mającego dostęp do lokalizacji źródłowej i lokalizacji replikacji.
4. W polu **Elementy do zreplikowania** wybierz archiwa lub lokalizacje kopii zapasowych do zreplikowania.
   Aby przełączać między archiwami i lokalizacjami, należy użyć przełącznika **Lokalizacje** / **Kopie zapasowe** widocznego w prawym górnym rogu ekranu.
   W przypadku wybierania wielu zaszyfrowanych archiwów muszą one mieć skonfigurowane to samo hasło szyfrowania. W przypadku archiwów używających różnych haseł szyfrowania należy utworzyć oddzielne plany.
5. W polu **Miejsce docelowe** określ lokalizację replikacji.
6. W polu **Jak przeprowadzić replikację** wybierz kopie zapasowe (nazywane równie punktami odzyskiwania) do replikacji.
   Dostępne są następujące opcje:
   - **Wszystkie kopie zapasowe**
   - **Tylko pełne kopie zapasowe**
   - **Tylko ostatnia kopia zapasowa**

   Dodatkowe informacje na temat tych opcji można znaleźć w sekcji "Elementy do zreplikowania" (s. 232).
7. W polu **Harmonogram** skonfiguruj harmonogram replikacji.
   W przypadku konfigurowania harmonogramu planu replikacji kopii zapasowych należy zadbać, aby ostatnia replikowana kopia zapasowa była wciąż dostępna w pierwotnej lokalizacji w momencie rozpoczęcia replikacji kopii zapasowych. Jeśli ta kopia zapasowa nie jest dostępna w pierwotnej lokalizacji, na przykład dlatego, że została usunięta przez regułę przechowywania, zostanie zreplikowane całe archiwum jako pełna kopia zapasowa. Może to być bardzo czasochłonne i zajmie dodatkowe miejsce w pamięci masowej.
8. W polu **Reguły przechowywania** określ reguły przechowywania dotyczące lokalizacji docelowej.
   Dostępne są następujące opcje:
   - **Według liczby kopii zapasowych**
   - **Według wieku kopii zapasowych** (osobne ustawienia dla miesięcznych, tygodniowych, dziennych i godzinowych kopii zapasowych)
   - **Według łącznego rozmiaru kopii zapasowych**

© Acronis International GmbH, 2003-2024

- **Przechowuj kopie zapasowe bezterminowo**

  Uwaga
  Wybranie tej opcji spowoduje zajęcie większej ilości miejsca w magazynie. Zbędne kopie zapasowe trzeba usuwać ręcznie.

9. [Jeśli w sekcji **Elementy do zreplikowania** wybrano archiwa zaszyfrowane] Włącz przełącznik **Hasło do kopii zapasowej**, a następnie podaj hasło szyfrowania.
10. [Opcjonalnie] Aby zmodyfikować opcje planu, kliknij ikonę koła zębatego, a następnie skonfiguruj opcje stosownie do potrzeb.
11. Kliknij **Utwórz**.

Elementy do zreplikowania

Uwaga
Niektóre operacje replikacji, na przykład replikacja całej lokalizacji lub wszystkich kopii zapasowych z zestawu kopii zapasowych, mogą być bardzo czasochłonne.

Replikacji można poddawać wybrane zestawy kopii zapasowych lub całe lokalizacje kopii zapasowych. W przypadku replikowania lokalizacji kopii zapasowych zostaną zreplikowane wszystkie znajdujące się w niej zestawy kopii zapasowych.

Zestawy kopii zapasowych składają się z kopii zapasowych (nazywanych równie punktami odzyskiwania). Trzeba wybrać kopie zapasowe, które mają zostać zreplikowane.

Dostępne są następujące opcje:

- **Wszystkie kopie zapasowe**
  Po każdym uruchomieniu planu replikacji są replikowane wszystkie kopie zapasowe z danego zestawu kopii zapasowych.
- **Tylko pełne kopie zapasowe**
  Replikowane są tylko pełne kopie zapasowe z danego zestawu kopii zapasowych.
- **Tylko ostatnia kopia zapasowa**
  Replikowana jest tylko najnowsza kopia zapasowa z danego zestawu kopii zapasowych — niezależnie od jej typu (pełna, różnicowa czy przyrostowa).

Wybierz opcję w zależności od potrzeb i używanego schematu tworzenia kopii zapasowych. Jeśli na przykład korzystasz ze schematu tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** i chcesz zreplikować tylko najnowszą przyrostową kopię zapasową, w planie replikacji kopii zapasowych wybierz **Tylko ostatnia kopia zapasowa**.

W poniższej tabeli podsumowano, które kopie zapasowe będą replikowane w przypadku różnych schematów tworzenia kopii zapasowych.

© Acronis International GmbH, 2003-2024

	Zawsze przyrostowa (jednoplikowa)	Zawsze pełne	Tygodniowe pełne, dzienne przyrostowe	Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe (GFS)
Wszystkie kopie zapasowe	Wszystkie kopie zapasowe z zestawu kopii zapasowych	Wszystkie kopie zapasowe z zestawu kopii zapasowych	Wszystkie kopie zapasowe z zestawu kopii zapasowych	Wszystkie kopie zapasowe z zestawu kopii zapasowych
Tylko pełne kopie zapasowe	Tylko pierwsza kopia zapasowa, czyli kopia pełna	Wszystkie kopie zapasowe	Jedna kopia zapasowa co tydzień*	Jedna kopia zapasowa co miesiąc*
Tylko ostatnia kopia zapasowa	Tylko najnowsza kopia zapasowa z zestawu kopii zapasowych*	Tylko najnowsza kopia zapasowa z zestawu kopii zapasowych*	Tylko najnowsza kopia zapasowa z zestawu kopii zapasowych, niezależnie od jej typu*	Tylko najnowsza kopia zapasowa z zestawu kopii zapasowych, niezależnie od jej typu*

*W przypadku konfigurowania harmonogramu planu replikacji kopii zapasowych należy zadbać, aby ostatnia replikowana kopia zapasowa była wciąż dostępna w pierwotnej lokalizacji w momencie rozpoczęcia replikacji kopii zapasowych. Jeśli ta kopia zapasowa nie jest dostępna w pierwotnej lokalizacji, na przykład dlatego, że została usunięta przez regułę przechowywania, zostanie zreplikowane całe archiwum jako pełna kopia zapasowa. Może to być bardzo czasochłonne i zajmie dodatkowe miejsce w pamięci masowej.

Obsługiwane lokalizacje

W poniższej tabeli podsumowano lokalizacje kopii zapasowych obsługiwane przez plany replikacji kopii zapasowej.

Lokalizacja kopii zapasowej	Obsługiwana jako źródło	Obsługiwana jako miejsce docelowe
Chmura	+	+
Folder lokalny	+	+
Folder sieciowy	+	+
Chmura publiczna	+	+
Folder NFS	–	–
Secure Zone	–	–

© Acronis International GmbH, 2003-2024

Sprawdzanie poprawności

Uwaga
Ta funkcja jest dostępna w ramach dzierżawców-klientów, dla których włączono limit **Zaawansowane kopie zapasowe — serwery** lub **Zaawansowane kopie zapasowe — NAS** w ramach pakietu Advanced Backup.

Sprawdzanie poprawności kopii zapasowej oznacza sprawdzanie, czy uda się odzyskać z niej dane.

Aby sprawdzić poprawność kopii zapasowej w ramach operacji przetwarzania danych poza hostem, należy utworzyć plan sprawdzania poprawności. Dodatkowe informacje na temat jego tworzenia można znaleźć w sekcji "Tworzenie planu sprawdzania poprawności" (s. 235).

Dostępne są następujące metody sprawdzania poprawności:

- Weryfikacja sumy kontrolnej
- Uruchom jako maszynę wirtualną
  - Puls maszyny wirtualnej
  - Sprawdzanie poprawności zrzutu ekranu

Można wybrać jedną lub więcej metod. W przypadku wybrania więcej niż jednej metody operacje poszczególnych metody sprawdzania poprawności są wykonywane po kolei. Dodatkowe informacje na temat tych metod można znaleźć w sekcji "Metody sprawdzania poprawności" (s. 238).

Sprawdzanie poprawności można wykonywać w odniesieniu do zestawów kopii zapasowych lub lokalizacji kopii zapasowych. Sprawdzanie poprawności lokalizacji kopii zapasowych oznacza sprawdzanie wszystkich znajdujących się w niej kopii zapasowych.

Obsługiwane lokalizacje

W poniższej tabeli przedstawiono obsługiwane lokalizacje kopii zapasowych i metody sprawdzania poprawności.

Uwaga
Opcja sprawdzanie poprawności nie jest dostępna w przypadku kopii zapasowych w chmurze publicznej ze względu na wygórowane koszty odczytu całego archiwum z chmury publicznej.

Lokalizacja kopii zapasowej	Weryfikacja sumy kontrolnej	Uruchom jako maszynę wirtualną	
		Puls maszyny wirtualnej	Sprawdzanie poprawności zrzutu ekranu
Chmura	+	+	+
Folder lokalny	+	+	+

© Acronis International GmbH, 2003-2024

Lokalizacja kopii zapasowej	Weryfikacja sumy kontrolnej	Uruchom jako maszynę wirtualną	
		Puls maszyny wirtualnej	Sprawdzanie poprawności zrzutu ekranu
Folder sieciowy	+	+	+
Folder NFS	–	–	–
Secure Zone	–	–	–

Status sprawdzanie poprawności

W przypadku pomyślnego wyniku sprawdzania poprawności kopia zapasowa zostaje oznaczona zieloną kropką i etykietą **Sprawdzono poprawność**.

Jeśli sprawdzanie poprawności zakończyło się niepowodzeniem, kopia zapasowa zostaje oznaczona czerwoną kropką. Sprawdzanie poprawności kończy się niepowodzeniem nawet w razie niepowodzenia tylko jednej z zastosowanych metod. Czasem może to być skutkiem niepoprawnej konfiguracji planu sprawdzania poprawności, na przykład zastosowania metody **Puls maszyny wirtualnej** do maszyn wirtualnych znajdujących się na niewłaściwym hoście.

Status sprawdzania poprawności kopii zapasowej jest aktualizowany po każdej nowej operacji sprawdzania poprawności. Status związany z poszczególnymi metodami sprawdzania poprawności jest aktualizowany osobno. Dlatego sprawdzanie poprawności kopii zapasowej, w ramach którego jedna metoda zakończyła się niepowodzeniem, będzie oznaczone jako zakończone niepowodzeniem, dopóki ta sama metoda sprawdzania poprawności nie zakończy się pomyślnie, nawet jeśli późniejsze operacje sprawdzania poprawności nie obejmowały metody zakończonej niepowodzeniem i mają pomyślny wynik.

Dodatkowe informacje na temat wyświetlania statusu sprawdzania poprawności można znaleźć w sekcji "Wyświetlanie statusu sprawdzania poprawności kopii zapasowej" (s. 241).

Tworzenie planu sprawdzania poprawności

Aby sprawdzić poprawność zestawu kopii zapasowych w ramach operacji przetwarzania danych poza hostem, należy utworzyć plan sprawdzania poprawności.

Aby utworzyć plan sprawdzania poprawności

1. W konsoli Cyber Protect kliknij **Zarządzanie** > **Sprawdzanie poprawności**.
2. Kliknij **Utwórz plan**.
   Zostanie otwarty szablon nowego planu sprawdzania poprawności.
3. [Opcjonalnie] Aby zmienić nazwę planu, kliknij nazwę domyślną.

© Acronis International GmbH, 2003-2024

4. W obszarze **Agent** wybierz agenta, który wykona sprawdzanie poprawności, a następnie kliknij **OK**.

   Aby przeprowadzić sprawdzanie poprawności przez uruchomienie maszyny wirtualnej z kopii zapasowej, wybierz komputer z agentem dla VMware lub agentem dla Hyper-V. W innych przypadkach można wybrać dowolny komputer mający dostęp do lokalizacji kopii zapasowej.
5. W polu **Elementy, których poprawność należy sprawdzić** wybierz zestawy kopii zapasowych, których poprawność chcesz sprawdzić.
   a. Wybierz zakres planu — pojedyncze zestawy kopii zapasowych lub całe lokalizacje — klikając **Lokalizacje** lub **Kopie zapasowe** w prawym górnym rogu.

      Jeśli wybrane kopie zapasowe są zaszyfrowane, wszystkie muszą używać tego samego hasła szyfrowania. W przypadku kopii zapasowych używających różnych haseł szyfrowania utwórz oddzielne plany.
   b. Kliknij **Dodaj**.
   c. W zależności od zakresu planu sprawdzania poprawności wybierz co najmniej jedną lokalizację i zestaw kopii zapasowych, a następnie kliknij **Gotowe**.
   d. Kliknij **Gotowe**.
6. W polu **Elementy do sprawdzenia poprawności** wybierz z wybranych zestawów kopii zapasowych kopie zapasowe (nazywane również punktami odzyskiwania), których poprawność ma zostać sprawdzona. Dostępne są następujące opcje:
   - **Wszystkie kopie zapasowe**
   - **Tylko ostatnia kopia zapasowa**
7. W polu **Jak sprawdzić poprawność** wybierz metodę sprawdzania poprawności.

   Możesz wybrać jedną z następujących opcji lub je obie:
   - **Weryfikacja sumy kontrolnej**
   - **Uruchom jako maszynę wirtualną**

   Dodatkowe informacje na temat tych metod można znaleźć w sekcji "Metody sprawdzania poprawności" (s. 238).
8. [W przypadku wybrania opcji **Weryfikacja sumy kontrolnej**] Kliknij **Gotowe**.
9. [W przypadku wybrania opcji **Uruchom jako maszynę wirtualną**]. Skonfiguruj ustawienia dla tej metody.
   a. W polu **Komputer docelowy** wybierz typ maszyny wirtualnej (ESXi lub Hyper-V), hosta oraz szablon nazwy maszyny, a następnie kliknij **OK**.

      Domyślna nazwa to **[Nazwa komputera]_sprawdzenie poprawności**.
   b. W polu **Magazyn danych** (w przypadku maszyny wirtualnej ESXi) lub **Ścieżka** (w przypadku maszyny wirtualnej Hyper-V) wybierz magazyn danych dla maszyny wirtualnej.
   c. Możesz wybrać jedną lub obie metody sprawdzania poprawności dostępne dzięki opcji **Uruchom jako maszynę wirtualną**:
      - **Puls maszyny wirtualnej**
      - **Sprawdzanie poprawności zrzutu ekranu**

© Acronis International GmbH, 2003-2024

d. [Opcjonalnie] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci oraz połączenia sieciowe maszyny wirtualnej.

   Domyślnie maszyna wirtualna nie jest podłączona do sieci, a wielkość pamięci maszyny wirtualnej jest równa wielkości pierwotnej maszyny.

e. Kliknij **Gotowe**.

10. [Opcjonalnie] W szablonie planu sprawdzania poprawności kliknij **Harmonogram** i skonfiguruj harmonogram.
11. [Jeśli zestawy kopii zapasowych wybrane w obszarze **Elementy, których poprawność należy sprawdzić** są zaszyfrowane] Włącz przełącznik **Hasło do kopii zapasowej**, a następnie podaj hasło szyfrowania.
12. [Opcjonalnie] Aby zmodyfikować opcje planu, kliknij ikonę koła zębatego.
13. Kliknij **Utwórz**.

W wyniku tych działań plan sprawdzania poprawności będzie gotowy i uruchamiany zgodnie ze skonfigurowanym harmonogramem. Aby niezwłocznie uruchomić plan, wybierz go w sekcji **Zarządzanie** > **Sprawdzanie poprawności**, a następnie kliknij **Uruchom teraz**.

Po uruchomieniu planu można sprawdzić bieżące działania i przejść do ich szczegółów w konsoli Cyber Protect w obszarze **Monitorowanie** > **Działania**.

Plan sprawdzania poprawności może obejmować wiele kopii zapasowych, a poprawność jednej kopii zapasowej może być sprawdzana w ramach wielu planów sprawdzania poprawności.

Uwaga
Wszystkie kopie zapasowe są przetwarzane po kolei, jedna po drugiej, przez jedno zadanie sprawdzania poprawności.

W przypadku agenta w danym czasie może być wykonywane tylko jedno zadanie sprawdzania poprawności. Różne zadania sprawdzania poprawności mogą być wykonywane jednocześnie pod warunkiem, że są wykonywane przez różnych agentów: dwa jednoczesne zadania wymagają dwóch agentów, trzy zadania — trzech agentów i tak dalej.

W poniższej tabeli zestawiono możliwe statusy sprawdzania poprawności.

Wynik działania	Plan z jedną kopią zapasową	Plan z wieloma kopiami zapasowymi
Powodzenie	Wszystkie metody sprawdzania poprawności zakończyły się wynikiem pomyślnym	Wszystkie metody sprawdzania poprawności zakończyły się wynikiem pomyślnym w przypadku wszystkich kopii zapasowych
Wykonano pomyślnie z ostrzeżeniami	N.d.	Co najmniej jedna metoda sprawdzania poprawności zakończyła się niepowodzeniem w przypadku co najmniej jednej kopii zapasowej
Niepowodzenie	Co najmniej jedna metoda sprawdzania poprawności zakończyła się niepowodzeniem	Co najmniej jedna metoda sprawdzania poprawności zakończyła się niepowodzeniem w przypadku wszystkich kopii zapasowych

© Acronis International GmbH, 2003-2024

Metody sprawdzania poprawności

W planie sprawdzania poprawności dostępne są następujące metody sprawdzania poprawności:

- Weryfikacja sumy kontrolnej
- Uruchom jako maszynę wirtualną
  - Puls maszyny wirtualnej
  - Sprawdzanie poprawności zrzutu ekranu

Weryfikacja sumy kontrolnej

Operacja sprawdzania poprawności metodą weryfikacji sumy kontrolnej polega na obliczeniu sumy kontrolnej każdego bloku danych, który można odzyskać z danej kopii zapasowej, a następnie porównaniu wyniku z oryginalną sumą kontrolną tego bloku danych, która została zapisana w ramach procesu tworzenia kopii zapasowej. Jedynym wyjątkiem jest sprawdzanie poprawności kopii zapasowych na poziomie plików znajdujących się w chmurze. Sprawdzanie poprawności tych kopii zapasowych polega na sprawdzaniu spójności zapisanych w nich metadanych.

Sprawdzanie poprawności metodą weryfikacji sumy kontrolnej jest czasochłonne — nawet w przypadku przyrostowych lub różnicowych kopii zapasowych, które nie są duże. Wynika to stąd, że w ramach sprawdzania poprawności są sprawdzane nie tylko dane fizycznie zawarte w przetwarzanej kopii zapasowej, ale wszystkie dane, które mają zostać odzyskane, co może oznaczać konieczność sprawdzenia poprawności również poprzednich kopii zapasowych.

Pomyślny wynik sprawdzenia poprawności metodą weryfikacji sumy kontrolnej oznacza wysokie prawdopodobieństwo odzyskania danych. Jednak w ramach sprawdzania poprawności tą metodą nie są sprawdzane wszystkie aspekty, które mają wpływ na proces odzyskiwania.

W przypadku kopii zapasowej systemu operacyjnego zalecamy zastosowanie niektórych z poniższych operacji dodatkowych:

- Odzyskiwanie testowe za pomocą nośnika startowego na zapasowy dysk twardy.
- Uruchomienie maszyny wirtualnej z kopii zapasowej w środowisku ESXi lub Hyper-V.
- Uruchomienie planu sprawdzania poprawności, w którym włączono metodę sprawdzania poprawności **Uruchom jako maszynę wirtualną**.

Uruchom jako maszynę wirtualną

Ta metoda działa tylko w przypadku kopii zapasowych na poziomie dysku, które obejmują system operacyjny. Aby skorzystać z tej metody, potrzebny jest host ESXi lub Hyper-V oraz zarządzający nim agent ochrony (agent dla VMware lub agent dla Hyper-V).

Metoda sprawdzania poprawności **Uruchom jako maszynę wirtualną** jest dostępna w następujących odmianach:

© Acronis International GmbH, 2003-2024

- Puls maszyny wirtualnej
- Sprawdzanie poprawności zrzutu ekranu

Trzeba wybrać co najmniej jedną z nich.

Puls maszyny wirtualnej

W ramach tej metody sprawdzania poprawności agent uruchamia maszynę wirtualną z kopii zapasowej, a następnie nawiązuje połączenie z oprogramowaniem VMware Tools lub Hyper-V Integration Services i sprawdza reakcję na badanie pulsu w celu uzyskania potwierdzenia, że system operacyjny został prawidłowo uruchomiony. Jeśli nie uda się nawiązać połączenia, agent będzie próbował się połączyć co dwie minuty, łącznie pięć razy. Jeśli żadna z prób nie zakończy się pomyślnie, sprawdzenie poprawności się nie powiedzie.

Niezależnie od liczby planów sprawdzania poprawności i kopii zapasowych, których poprawność jest sprawdzana, agent dokonujący sprawdzenia poprawności uruchamia maszyny wirtualne pojedynczo. Gdy tylko wynik sprawdzania poprawności będzie znany, agent usunie daną maszynę wirtualną i uruchomi następną.

Uwaga
Metody tej należy używać tylko do sprawdzania poprawności kopii zapasowych maszyn wirtualnych VMware przez uruchamianie tych kopii jako maszyn wirtualnych na hoście ESXi, a także kopii zapasowych maszyn wirtualnych Hyper-V przez uruchamianie ich jako maszyn wirtualnych na hoście Hyper-V.

Sprawdzanie poprawności zrzutu ekranu

W ramach tej metody sprawdzania poprawności agent uruchamia maszynę wirtualną z kopii zapasowej, a podczas uruchamiania maszyny wirtualnej wykonywane są zrzuty ekranu. Moduł inteligencji maszyn (machine intelligence, MI) sprawdza zrzuty ekranu, a gdy wykryje na nich ekran logowania, oznacza kopię zapasową jako „Sprawdzono poprawność”.

Zrzut ekranu zostaje załączony do punktu odzyskiwania i można go pobrać na poziomie konsoli Cyber Protect w ciągu roku od ukończenia sprawdzania poprawności. Dodatkowe informacje o sprawdzaniu zrzutu ekranu można znaleźć w sekcji "Wyświetlanie statusu sprawdzania poprawności kopii zapasowej" (s. 241).

Jeśli na Twoim koncie użytkownika zostały włączone powiadomienia, otrzymasz wiadomość e-mail o statusie sprawdzania poprawności kopii zapasowej z załączonym zrzutem ekranu. Dodatkowe informacje na temat tych powiadomień można znaleźć w sekcji Zmienianie ustawień powiadomień dla użytkownika.

Sprawdzanie poprawności zrzutu ekranu jest obsługiwane przez agenty w wersji 15.0.30971 (wydanej w listopadzie 2022 roku) lub nowszej.

© Acronis International GmbH, 2003-2024

Uwaga
Sprawdzanie poprawności zrzutu ekranu działa najlepiej w przypadku kopii zapasowych systemu Windows, a także systemu Linux z ekranem logowania w graficznym interfejsie użytkownika. Nie jest to metoda optymalna w przypadku systemów Linux z ekranem logowania z konsoli.

Zmienianie limitu czasu pulsu maszyny wirtualnej i sprawdzania poprawności zrzutu ekranu

W przypadku sprawdzania poprawności kopii zapasowej przez uruchomienie jej jako maszyny wirtualnej można skonfigurować limit czasu między uruchomieniem maszyny wirtualnej a wysłaniem zapytania o puls lub wykonaniem zrzutu ekranu.

Domyślnie jest stosowany następujący odstęp czasowy:

- Jedna minuta — w przypadku kopii zapasowych przechowywanych w folderze lokalnym lub udziale sieciowym.
- Pięć minut — w przypadku kopii zapasowych przechowywanych w chmurze.

Można to zmienić, edytując plik konfiguracyjny agenta dla VMware lub agenta dla Hyper-V.

Aby zmienić limit czasu

1. Otwórz plik konfiguracyjny do edycji. Plik ten można znaleźć w następujących lokalizacjach:
   - W przypadku agenta dla VMware lub agenta dla Hyper-V działającego w systemie Windows: `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - W przypadku agenta dla VMware (urządzenie wirtualne): `/bin/mms_settings.config`
     Dodatkowe informacje na temat dostępu do pliku konfiguracyjnego na urządzeniu wirtualnym można znaleźć w sekcji "Połączenia SSH z urządzeniem wirtualnym" (s. 179).
2. Przejdź do sekcji `<validation>` i odpowiednio do potrzeb zmień wartości dla kopii zapasowych przechowywanych lokalnie i w chmurze:

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. Zapisz plik konfiguracyjny.
4. Uruchom ponownie agenta.
   - [W przypadku agenta dla VMware lub agenta dla Hyper-V działającego w systemie Windows] Uruchom w wierszu polecenia następujące polecenia:

```
net stop mms
```


© Acronis International GmbH, 2003-2024

```
net start mms
```

- [W przypadku agenta dla VMware (urządzenie wirtualne)] Uruchom ponownie maszynę wirtualną z agentem.

Konfigurowanie liczby ponownych prób w przypadku wystąpienia błędu

Aby zmaksymalizować liczbę pomyślnie wykonanych operacji sprawdzania poprawności, można skonfigurować automatyczne ponawianie prób w przypadku operacji zakończonych błędem.

Aby skonfigurować automatyczne ponawianie prób

1. Podczas tworzenia planu sprawdzania poprawności kliknij ikonę koła zębatego.
2. W panelu **Opcje** wybierz **Obsługa błędów**.
3. W obszarze **W przypadku wystąpienia błędu spróbuj ponownie** kliknij **Tak**.
4. W polu **Liczba prób** skonfiguruj maksymalną liczbę ponownych prób, które mają zostać podjęte w przypadku wystąpienia błędu.

   Operacja sprawdzania poprawności będzie uruchamiana ponownie do czasu, aż zostanie pomyślnie ukończona, lub do osiągnięcia progu maksymalnej liczby ponownych prób.
5. W polu **Odstęp między próbami** skonfiguruj odstęp czasowy między dwiema kolejnymi próbami.
6. Kliknij **Gotowe**.

Wyświetlanie statusu sprawdzania poprawności kopii zapasowej

Status sprawdzania poprawności kopii zapasowej można wyświetlić na karcie **Urządzenia** lub karcie **Magazyn kopii zapasowych**.

Można też zobaczyć status każdej metody sprawdzania poprawności i pobrać zrzut ekranu wykonany w ramach metody sprawdzania poprawności zrzutu ekranu.

Dodatkowe informacje na temat działania statusów można znaleźć w sekcji "Status sprawdzanie poprawności" (s. 235).

Aby wyświetlić status sprawdzania poprawności kopii zapasowej

Urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz obciążenie, w którego przypadku chcesz wyświetlić status sprawdzania poprawności kopii zapasowej, i kliknij **Odzyskiwanie**.
3. [Jeśli jest dostępna więcej niż jedna lokalizacja kopii zapasowych] Wybierz lokalizację kopii zapasowych.
4. Wybierz kopię zapasową, której status chcesz wyświetlić.

Magazyn kopii zapasowych

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych**.
2. Wybierz lokalizację, w której jest przechowywany zestaw kopii zapasowych.
3. Wybierz zestaw kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
4. Wybierz kopię zapasową, której status sprawdzania poprawności chcesz wyświetlić.

Czyszczenie

Czyszczenie to operacja polegająca na usunięciu nieaktualnych kopii zapasowych zgodnie z regułami przechowywania. Ta operacja dotyczy tylko agentów i obciążeń, a nie kopii zapasowych z chmury do chmury (które można usunąć tylko ręcznie).

Uwaga
Ta funkcja jest dostępna w ramach dzierżawców-klientów, dla których włączono limit **Zaawansowane kopie zapasowe — serwery** lub **Zaawansowane kopie zapasowe — NAS** w ramach pakietu Advanced Backup.

Obsługiwane lokalizacje

Plany czyszczenia obejmują wszystkie lokalizacje kopii zapasowych, z wyjątkiem folderów NFS i partycji Secure Zone.

Aby utworzyć plan czyszczenia

1. W konsoli Cyber Protect kliknij **Zarządzanie** > **Czyszczenie**.
2. Kliknij **Utwórz plan**.
3. W polu **Agent** wybierz agenta, który wykona czyszczenie.
   Możesz wybrać dowolnego agenta mającego dostęp do danej lokalizacji kopii zapasowych.
4. W polu **Elementy do wyczyszczenia** wybierz archiwa lub lokalizacje kopii zapasowych do wyczyszczenia.
   Aby przełączać między archiwami i lokalizacjami, należy użyć przełącznika **Lokalizacje** / **Kopie zapasowe** widocznego w prawym górnym rogu ekranu.
   W przypadku wybierania wielu zaszyfrowanych archiwów muszą one mieć skonfigurowane to samo hasło szyfrowania. W przypadku archiwów używających różnych haseł szyfrowania należy utworzyć oddzielne plany.
5. W polu **Harmonogram** skonfiguruj harmonogram czyszczenia.
6. W polu **Reguły przechowywania** określ reguły przechowywania.
   Dostępne są następujące opcje:
   - **Według liczby kopii zapasowych**
   - **Według wieku kopii zapasowych** (osobne ustawienia dla miesięcznych, tygodniowych, dziennych i godzinowych kopii zapasowych)
   - **Według łącznego rozmiaru kopii zapasowych**

© Acronis International GmbH, 2003-2024

7. [Jeśli w sekcji **Elementy do zreplikowania** wybrano archiwa zaszyfrowane] Włącz przełącznik **Hasło do kopii zapasowej**, a następnie podaj hasło szyfrowania.
8. [Opcjonalnie] Aby zmodyfikować opcje planu, kliknij ikonę koła zębatego, a następnie skonfiguruj opcje stosownie do potrzeb.
9. Kliknij **Utwórz**.

Konwersja na maszynę wirtualną

Konwersja na maszynę wirtualną jest możliwa tylko dla kopii zapasowych na poziomie dysku. Jeśli kopia zapasowa obejmuje wolumin systemowy i zawiera wszystkie informacje potrzebne do uruchomienia systemu operacyjnego, wynikowa maszyna wirtualna może się uruchomić samodzielnie. W przeciwnym razie jej dyski wirtualne można dodać do innej maszyny wirtualnej.

Uwaga
Nie można tworzyć kopii zapasowych maszyn wirtualnych replikowanych za pomocą natywnej funkcji replikacji maszyn wirtualnych Scale Computing.

Można utworzyć osobny plan konwersji na maszynę wirtualną i uruchomić go ręcznie lub według harmonogramu.

Informacje na temat wymagań wstępnych i ograniczeń można znaleźć w sekcji "Co trzeba wiedzieć o konwersji" (s. 245).

Uwaga
Ta funkcja jest dostępna w ramach dzierżawców-klientów, dla których włączono limit **Zaawansowane kopie zapasowe — serwery** lub **Zaawansowane kopie zapasowe — NAS** w ramach pakietu Advanced Backup.

Aby utworzyć plan konwersji na maszynę wirtualną

1. Kliknij **Zarządzanie** > **Konwersja na maszynę wirtualną**.
2. Kliknij **Utwórz plan**.
   Program wyświetli szablon nowego planu.
3. [Opcjonalnie] Aby zmienić nazwę planu, kliknij nazwę domyślną.
4. W obszarze **Konwertuj na** wybierz typ docelowej maszyny wirtualnej. **Można wybrać jedną z następujących opcji**:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**

© Acronis International GmbH, 2003-2024

- **Pliki VHDX**

Uwaga
W celu oszczędzania miejsca w pamięci masowej każda konwersja na pliki VHDX lub VMware Workstation powoduje zastąpienie w lokalizacji docelowej plików VHDX/VMDK utworzonych podczas poprzedniej konwersji.

5. Wykonaj jedną z następujących czynności:
   - [W przypadku maszyn VMware ESXi, Hyper-V i Scale Computing HC3] Kliknij **Host**, wybierz host docelowy, a następnie określ szablon nazw nowych maszyn.
   - [W przypadku maszyn wirtualnych innego typu] W polu **Ścieżka** wskaż miejsce zapisu oraz szablon nazw plików maszyn wirtualnych.

   Domyślna nazwa to **[Nazwa komputera]_skonwertowany**.
6. Kliknij **Agent** i wybierz agenta, który ma przeprowadzić konwersję.
7. Kliknij **Elementy do przekonwertowania** i wybierz kopie zapasowe, które zostaną przekonwertowane na maszyny wirtualne w ramach tego planu.

   Możesz przełączać między wybieraniem kopii zapasowych a wybieraniem całych lokalizacji przy użyciu przełącznika **Lokalizacje**/**Kopie zapasowe** w prawym górnym rogu.

   Jeśli wybrane kopie zapasowe są zaszyfrowane, wszystkie muszą używać tego samego hasła szyfrowania. W przypadku kopii zapasowych używających różnych haseł szyfrowania utwórz oddzielne plany.
8. [Tylko w przypadku maszyn VMware ESXi i Hyper-V] Kliknij **Magazyn danych** w przypadku maszyny ESXi lub **Ścieżka** w przypadku maszyny Hyper-V, a następnie wybierz magazyn danych (magazyn) dla maszyny wirtualnej.
9. [Tylko w przypadku maszyn wirtualnych VMware ESXi i Hyper-V] Wybierz tryb alokowania dysku. Ustawienie domyślne to **Elastyczne** dla VMware ESXi i **Powiększający się dynamicznie** dla Hyper-V.
10. [Opcjonalnie] [W przypadku maszyn wirtualnych VMware ESXi, Hyper-V Scale Computing HC3] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów lub połączenia sieciowe maszyny wirtualnej.
11. [Opcjonalnie] Kliknij **Harmonogram**, a następnie zmień harmonogram.
12. Jeśli kopie zapasowe wybrane w sekcji **Elementy do przekonwertowania** są zaszyfrowane, włącz przełącznik **Hasło do kopii zapasowej**, a następnie podaj hasło szyfrowania. W przeciwnym razie pomiń ten krok.
13. [Opcjonalnie] Aby zmodyfikować opcje planu, kliknij ikonę koła zębatego.
14. Kliknij **Utwórz**.

© Acronis International GmbH, 2003-2024

Co trzeba wiedzieć o konwersji

Obsługiwane typy maszyn wirtualnych

Konwersja kopii zapasowej na maszynę wirtualną może zostać wykonana przez tego samego agenta, który utworzył kopię zapasową, lub innego.

Aby dokonać konwersji na maszynę VMware ESXi, Hyper-V lub Scale Computing HC3, potrzebny jest odpowiednio host ESXi, Hyper-V lub Scale Computing HC3 oraz zarządzający nim agent ochrony (agent dla VMware, agent dla Hyper-V lub agent dla Scale Computing HC3).

Konwersja na pliki VHDX jest wykonywana przy założeniu, że pliki zostaną podłączone do maszyny wirtualnej Hyper-V jako dyski wirtualne.

Poniższa tabela zawiera zestawienie typów maszyn wirtualnych, które można utworzyć za pomocą operacji **Konwertuj na maszynę wirtualną**. Wiersze w tabeli zawierają typ konwertowanych maszyn wirtualnych. Kolumny zawierają agenty, które dokonują konwersji.

Typ maszyny wirtualnej	Agent dla VMware	Agent dla Hyper-V	Agent dla systemu Windows	Agent dla systemu Linux	Agent dla systemu Mac	Agent dla Scale Computing HC3	Agent dla oVirt (KVM)	Agent dla Virtuozzo Hybrid Infrastructure	Agent dla Virtuozzo
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware Workstation	+	+	+	+	–	–	–	–	–
Pliki VHDX	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

© Acronis International GmbH, 2003-2024

Ograniczenia

- Kopii zapasowych przechowywanych w udziale NFS nie można konwertować.
- Kopie zapasowe przechowywane na partycji Secure Zone mogą być konwertowane tylko przez agenta działającego na tym samym komputerze.
- Kopie zapasowe zawierające woluminy logiczne systemu Linux (LVM) można konwertować tylko wtedy, gdy zostały utworzone przez agenta dla VMware, agenta dla Hyper-V lub agenta dla Scale Computing HC3 i są kierowane do tego samego hiperwizora. Konwersja między hiperwizorami nie jest obsługiwana.
- W przypadku konwertowania kopii zapasowych komputera z systemem Windows na maszynę wirtualną VMware Workstation lub pliki VHDX wynikowa maszyna wirtualna dziedziczy typ procesora po komputerze dokonującym konwersji. W związku z tym w systemie operacyjnym-gościu są instalowane odpowiednie sterowniki procesora. W przypadku uruchomienia na hoście z procesorem innego typu system-gość wyświetla błąd sterownika. Sterownik należy zaktualizować ręcznie.

Konwersja regularna na maszynę wirtualną a uruchamianie maszyny wirtualnej z kopii zapasowej

Obie operacje zapewniają maszynę wirtualną, którą można uruchomić w czasie liczonym w sekundach, jeśli oryginalna maszyna ulegnie awarii.

Konwersja regularna na maszynę wirtualną oznacza wykorzystywanie zasobów procesora i pamięci. Pliki maszyny wirtualnej stale zajmują miejsce w magazynie danych (pamięci masowej). Jeśli w celu konwersji posłużono się hostem produkcyjnym, może to być niepraktyczne. Wydajność maszyny wirtualnej jednak jest ograniczona tylko przez zasoby hosta.

Uruchomienie maszyny wirtualnej z kopii zapasowej powoduje obciążenie zasobów tylko w czasie działania maszyny wirtualnej. Miejsce w magazynie danych (pamięci masowej) jest potrzebne tylko do przechowywania zmian zachodzących na dyskach wirtualnych. Maszyna wirtualna może jednak działać wolniej, ponieważ komputer nie ma bezpośredniego dostępu do dysków wirtualnych, tylko komunikuje się z agentem, który odczytuje dane z kopii zapasowej. Ponadto ta maszyna wirtualna jest tymczasowa.

Zasady działania konwersji regularnej na maszynę wirtualną

Sposób działania konwersji regularnej zależy od wybranego miejsca, w którym ma zostać utworzona maszyna wirtualna.

- **W przypadku wybrania opcji zapisu maszyny wirtualnej w postaci zestawu plików:** każda konwersja powoduje ponowne utworzenie tej maszyny od podstaw.
- **Po wybraniu opcji tworzenia maszyny wirtualnej na serwerze wirtualizacji:** w przypadku konwersji przyrostowej lub różnicowej kopii zapasowej program nie tworzy ponownie maszyny wirtualnej, tylko przyrostowo aktualizuje już istniejącą maszynę. Taka konwersja trwa zwykle krócej. Wymaga ona przesłania przez sieć mniejszej ilości danych i mniej obciąża procesor hosta

© Acronis International GmbH, 2003-2024

wykonującego konwersję. Jeśli aktualizacja maszyny wirtualnej nie jest możliwa, program utworzy ją od podstaw.

Poniżej zamieszczono szczegółowy opis obu tych przypadków.

Po wybraniu opcji zapisu maszyny wirtualnej w postaci zestawu plików

W wyniku pierwszej konwersji tworzona jest nowa maszyna wirtualna. Każda kolejna konwersja powoduje ponowne utworzenie tej maszyny od podstaw. Najpierw tymczasowo zmieniana jest nazwa starej maszyny. Następnie program tworzy nową maszynę wirtualną o takiej samej nazwie, jak poprzednia nazwa starej maszyny. Jeśli operacja ta zakończy się powodzeniem, program usuwa starą maszynę. Jeśli operacja ta zakończy się niepowodzeniem, program usuwa nową maszynę i przywraca poprzednią nazwę starej maszynie. Oznacza to, że rezultatem konwersji zawsze jest jedna maszyna wirtualna. Jednak podczas konwersji wymagane jest dodatkowe miejsce, tak aby zmieściła się także stara maszyna.

Po wybraniu opcji tworzenia maszyny wirtualnej na serwerze wirtualizacji

Pierwsza konwersja spowoduje utworzenie nowej maszyny wirtualnej. Każda kolejna zadziała zgodnie z następującą zasadą:

- Jeśli od czasu ostatniej konwersji została utworzona *pełna kopia zapasowa*, maszyna wirtualna zostanie ponownie utworzona od podstaw, tak jak opisano wcześniej w tej sekcji.
- W innym przypadku istniejąca maszyna wirtualna zostanie zaktualizowana zgodnie ze zmianami dokonanymi od czasu ostatniej konwersji. Jeśli aktualizacja nie będzie możliwa (na przykład usunięto migawki pośrednie — zobacz poniżej), maszyna wirtualna zostanie utworzona ponownie od podstaw.

Migawki pośrednie

Aby można było bezpiecznie zaktualizować przekonwertowaną maszynę wirtualną, program przechowuje migawkę pośrednią hiperwizora tej maszyny. Migawka ma nazwę rozpoczynającą się od **Replica...** i musi zostać zachowana.

Migawka **Replica...** odpowiada wynikowi ostatniej konwersji. Można z niej skorzystać w celu przywrócenia maszyny do danego stanu, na przykład do odrzucenia wprowadzonych zmian po zakończeniu pracy z maszyną.

W przypadku przekonwertowanych maszyn wirtualnych Scale Computing HC3 jest tworzona dodatkowa **Migawka użytkowa**. Korzysta z niej tylko usługa Cyber Protection.

Plany skanowania kopii zapasowych

Aby przeskanować kopie zapasowe pod kątem złośliwego oprogramowania (w tym ransomware), utwórz plan skanowania kopii zapasowych.

© Acronis International GmbH, 2003-2024

Ważne
Plany skanowania kopii zapasowych nie są obsługiwane w przypadku wszystkich obciążeń i magazynów kopii zapasowych. Szczegółowe informacje można znaleźć w artykule "Ograniczenia" (s. 924).

Aby utworzyć plan skanowania kopii zapasowych

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Skanowanie kopii zapasowych**.
2. Kliknij **Utwórz plan**.
3. Określ nazwę planu i następujące parametry:
   - **Typ skanowania**:
     - **Chmura** — definicji tej opcji nie można zmienić. Skanowanie kopii zapasowych zostanie wykonane przez automatycznie wybranego agenta w chmurze.
   - **Kopie zapasowe do przeskanowania**:
     - **Lokalizacje** — wybierz lokalizacje z zestawami kopii zapasowych do przeskanowania.
     - **Kopie zapasowe** — wybierz zestawy kopii zapasowych do przeskanowania.
   - **Cel skanowania**:
     - **Złośliwe oprogramowanie** — definicji tej opcji nie można zmienić. W ramach skanowania wybrane zestawy kopii zapasowych zostaną sprawdzone pod kątem złośliwego oprogramowania (w tym ransomware).
   - **Szyfrowanie** — aby przeskanować zestawy zaszyfrowanych kopii zapasowych, należy podać hasło szyfrowania. Jeśli zostanie wybrana lokalizacja lub wiele zestawów kopii zapasowych, a podane hasło nie będzie odpowiednie w przypadku któregoś zestawu, zostanie utworzony alert.
   - **Harmonogram** — definicji tej opcji nie można zmienić. W chmurze skanowanie rozpocznie się automatycznie.
4. Kliknij **Utwórz**.

W związku z tym zostanie utworzony plan skanowania kopii zapasowych, a agent w chmurze przeskanuje wskazane przez użytkownika lokalizacje lub zestawy kopii zapasowych w poszukiwaniu złośliwego oprogramowania.

Plany tworzenia kopii zapasowych aplikacji w chmurze

Na karcie **Zarządzanie** > **Kopia zapasowa aplikacji w chmurze** wyświetlane są plany tworzenia kopii zapasowych z chmury do chmury. W ramach tych planów tworzone są kopie zapasowe aplikacji działających w chmurze za pomocą agentów, które działają w chmurze i używają chmury jako lokalizacji kopii zapasowych.

W tej sekcji można wykonywać następujące operacje:

- Tworzenie, wyświetlanie, uruchamianie, zatrzymywanie, edytowanie i usuwanie planu tworzenia kopii zapasowych

© Acronis International GmbH, 2003-2024

- Wyświetlanie działań związanych z poszczególnymi planami tworzenia kopii zapasowych
- Wyświetlanie alertów związanych z poszczególnymi planami tworzenia kopii zapasowych

Więcej informacji o kopiach zapasowych aplikacji w chmurze można znaleźć w sekcjach:

- Ochrona danych Microsoft 365
- Ochrona danych pakietu Google Workspace

Ręczne uruchamianie operacji tworzenia kopii zapasowej z chmury do chmury

Aby zapobiec zakłóceniom działania usługi Cyber Protection, liczbę operacji ręcznego tworzenia kopii zapasowych z chmury do chmury ograniczono do 10 na organizację Microsoft 365 lub Google Workspace w ciągu godziny. Po osiągnięciu tej liczby dopuszczalna liczba operacji jest resetowana do jednej na godzinę, a następnie co godzinę udostępniana jest dodatkowa operacja (np. godzina 1 — 10 operacji, godzina 2 — 1 operacja, godzina 3 — 2 operacje), aż do osiągnięcia łącznie 10 operacji na godzinę.

Planów tworzenia kopii zapasowych stosowanych do grup urządzeń (skrzynek pocztowych, dysków, witryn) lub obejmujących więcej niż 10 urządzeń nie można uruchamiać ręcznie.

Ochrona aplikacji do współpracy i komunikacji

Obecnie powszechnie używa się aplikacji Zoom, Cisco Webex Meetings, Citrix Workspace i Microsoft Teams do wideokonferencji / konferencji internetowych i komunikacji. Usługa Cyber Protection umożliwia chronienie narzędzi do współpracy.

Proces konfiguracji ochrony aplikacji Zoom, Cisco Webex Meetings, Citrix Workspace i Microsoft Teams wygląda podobnie. Poniżej opisano konfigurację ochrony na przykładzie aplikacji Zoom.

Aby skonfigurować ochronę aplikacji Zoom

1. Na komputerze, na którym jest zainstalowana aplikacja do współpracy, zainstaluj agenta ochrony.
2. Zaloguj się do konsoli Cyber Protect i zastosuj plan ochrony, w którym jest włączony jeden z następujących modułów:
   - **Ochrona przed wirusami i złośliwym oprogramowaniem** (z włączonymi funkcjami **Ochrona własna** i **Active Protection**) — jeśli masz jedną z wersji Cyber Protect.
   - **Active Protection** (z włączoną funkcją **Ochrona własna**) — jeśli masz jedną z wersji Cyber Backup.
3. [Opcjonalnie] Aby aktywować automatyczną instalację aktualizacji, skonfiguruj moduł **Zarządzanie poprawkami** w planie ochrony.

W wyniku tego aplikacja Zoom zostanie objęta ochroną, w której ramach są wykonywane następujące czynności:

© Acronis International GmbH, 2003-2024

- Automatyczne instalowanie aktualizacji klienta Zoom
- Ochrona procesów aplikacji Zoom przed wstrzyknięciem kodu
- Blokowanie podejrzanych operacji procesów aplikacji Zoom
- Chronienie plików „hosts” przed dodawaniem domen związanych z aplikacją Zoom

© Acronis International GmbH, 2003-2024

Poznanie bieżącego poziomu ochrony

Monitorowanie

Karta **Monitorowanie** udostępnia ważne informacje o aktualnym poziomie ochrony i zawiera następujące pulpity nawigacyjne:

- **Przegląd**
- **Działania**
- **Alerty**
- **Kanał dotyczący zagrożeń** (dodatkowe informacje można znaleźć w sekcji "Kanał dotyczący zagrożeń" (s. 297))

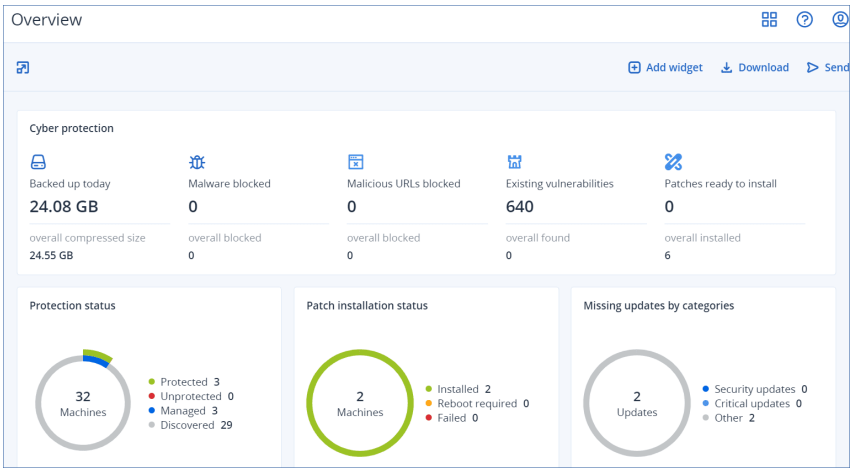
Pulpit nawigacyjny Przegląd

Pulpit nawigacyjny **Przegląd** udostępnia szereg dostosowywalnych widżetów zapewniających ogólny obraz operacji związanych z usługą Cyber Protection. Widżety dla pozostałych usług będą dostępne w przyszłych wersjach.

Widżety są aktualizowane co 5 minut. Widżety mają klikalne elementy, które pozwalają badać i rozwiązywać problemy. Możesz pobrać bieżący stan pulpitu nawigacyjnego lub przesłać go za pomocą poczty e-mail w formacie .pdf oraz/lub .xlsx.

Możesz wybierać spośród różnorodnych widżetów przedstawianych w formie tabel, wykresów kołowych, wykresów słupkowych, list i map drzew. Możesz dodać wiele widżetów tego samego typu, ale z różnymi filtrami.

Przyciski **Pobierz** i **Wyślij** w sekcji **Monitorowanie** > **Przegląd** są niedostępne w wersjach Standard usługi Cyber Protection.



Aby zmienić ustawienie widżetów na pulpicie nawigacyjnym

Klikaj nazwy widżetów i zmieniaj ich ustawienie metodą „przeciągnij i upuść”.

Aby edytować widżet

© Acronis International GmbH, 2003-2024

Kliknij ikonę ołówka obok nazwy widżetu. Edycja widżetu pozwala zmienić jego nazwę, zmodyfikować zakres czasu, ustawić filtry i pogrupować wiersze.

Aby dodać widżet

Kliknij **Dodaj widżet** i wykonaj jedną z następujących czynności:

- Kliknij widżet, który chcesz dodać. Widżet zostanie dodany z domyślnymi ustawieniami.
- Aby edytować widżet przed dodaniem, zaznacz go i kliknij Dostosuj. Po skończonej edycji widżetu kliknij **Gotowe**.

Aby usunąć widżet

Kliknij symbol X obok nazwy widżetu.

Pulpit nawigacyjny Działania

Pulpit nawigacyjny **Działania** zawiera przegląd bieżących i przeszłych działań. Domyślny okres przechowywania to 90 dni.

Aby dostosować widok pulpitu nawigacyjnego **Działania**, kliknij ikonę koła zębatego i wybierz kolumny do wyświetlenia.

Aby móc sprawdzać postęp działań w czasie rzeczywistym, zaznacz pole wyboru **Odświeżaj automatycznie**. Pamiętaj jednak, że częste aktualizowanie wielu działań pogarsza wydajność serwera zarządzania.

Listę działań można przeszukiwać według następujących kryteriów:

- **Nazwa urządzenia**
  To jest nazwa komputera, na którym jest wykonywane dane działanie.
- **Rozpoczęte przez**
  To jest konto, które rozpoczęło dane działanie.

Działania można też filtrować według następujących właściwości:

- **Status**
  Na przykład wykonane pomyślnie, niepowodzenie, w toku itd.
- **Typ**
  Na przykład stosowanie planu, usuwanie kopii zapasowych, instalowanie aktualizacji oprogramowania.
- **Czas**
  Na przykład ostatnie działania, działania z ostatnich 24 godzin lub działania we wskazanym okresie w ramach domyślnego okresu przechowywania.

Aby zobaczyć więcej informacji o jakimś działaniu, wybierz je z listy, a następnie na panelu **Szczegóły działania** kliknij **Wszystkie właściwości**. Dodatkowe informacje na temat dostępnych właściwości można znaleźć w opisach interfejsów API Działanie i Zadanie w portalu Developer Network Portal.

© Acronis International GmbH, 2003-2024

Pulpit nawigacyjny Alerty

Na pulpicie nawigacyjnym **Alerty** są wyświetlane wszystkie aktualne alerty. Wymienione alerty to alerty krytyczne lub alerty o błędach związane zwykle z zadaniami, na przykład tworzeniem kopii zapasowych, które z jakichś powodów się nie powiodły.

Aby przefiltrować alerty na pulpicie nawigacyjnym

1. Z listy rozwijanej **Widok** wybierz jedne z następujących kryteriów:
   - **Istotność alertu**
   - **Kategoria alertów**
   - **Typ alertu**
   - **Typ monitorowania**
   - **Zakres dat: od ... do ...**
   - **Obciążenie**
   - **Plan**
   - **Klient**
2. Jeśli z listy rozwijanej **Kategoria** została wybrana opcja **Kategoria alertów**, należy wybrać konkretną kategorię do wyświetlenia.
3. Jeśli chcesz wyświetlić wszystkie alerty bez ich filtrowania, kliknij **Wszystkie typy alertów**.

W ramach każdego alertu można wykonywać następujące czynności:

- Uzyskać dostęp do urządzenia, którego dotyczy alert, przez kliknięcie łącza **Urządzenia**.
- Przeczytać i spróbować się zastosować do porad przedstawionych w sekcji **Rozwiązywanie problemów** alertu.
- Uzyskać dostęp do odpowiedniej dokumentacji i artykułów z bazy wiedzy, klikając **Szukaj rozwiązania**. Funkcja **Szukaj rozwiązania** uzupełni zapytanie aktualnymi szczegółami alertu, aby jak najefektywniej Ci pomóc.

Aby posortować alerty na pulpicie nawigacyjnym

W tabeli alertów kliknij przycisk strzałki obok jednej z następujących nazw kolumn:

- **Istotność alertu**
- **Typ alertu**
- **Utworzono**
- **Kategoria alertów**
- **Obciążenie**
- **Plan**

© Acronis International GmbH, 2003-2024

Typy alertów

Będą generowane alerty następujących typów:

- Alerty dotyczące kopii zapasowych
- Alerty dotyczące odzyskiwania po awarii
- Alerty dotyczące ochrony przed złośliwym oprogramowaniem
- Alerty dotyczące licencjonowania
- Alerty dotyczące modułu Filtrowanie adresów URL
- Alerty dotyczące modułu EDR
- Alerty związane z kontrolą urządzeń
- Alerty dotyczące systemu

Alerty dotyczące kopii zapasowych

Alert	Opis	Jak obsłużyć alert
Utworzenie kopii zapasowej się nie powiodło	Alert jest generowany, gdy operacja tworzenia kopii zapasowej się nie powiodła z powodu możliwego do usunięcia błędu lub została przerwana z powodu wyłączenia systemu.	Sprawdź dziennik operacji tworzenia kopii zapasowej: kliknij maszynę, aby ją zaznaczyć, kliknij **Działania**, a następnie znajdź ostrzeżenie w dzienniku. Komunikat powinien sygnalizować główną przyczynę problemu.
Kopia zapasowa została utworzona z ostrzeżeniami	Alert jest generowany, gdy operacja tworzenia kopii zapasowej się powiodła, ale z ostrzeżeniami.	Sprawdź dzienniki konwersji na maszynę wirtualną, replikacji lub planów sprawdzania poprawności. Problemy występujące podczas tych operacji generują alerty „Działanie się nie powiodło” lub „Działanie ukończone z ostrzeżeniem”.
Tworzenie kopii zapasowej zostało anulowane	Alert jest generowany po każdym ręcznym anulowaniu operacji tworzenia kopii zapasowej.	Można ręcznie uruchomić operację tworzenia kopii zapasowej, klikając **Uruchom teraz**, albo poczekać, aż zostanie ona uruchomiona w następnym zaplanowanym terminie.
Operacja tworzenia kopii zapasowej anulowana z powodu zamkniętego okna na utworzenie kopii zapasowej	Alert jest generowany w przypadku pominięcia działania związanego z tworzeniem kopii zapasowej, ponieważ nie zmieściło się ono w oknie określonym w opcjach	Zmień konfigurację harmonogramu lub edytuj opcje planu tworzenia kopii zapasowych w sekcji **Wydajność i okno na utworzenie kopii zapasowej**. Rozwiń sekcję z produktem, aby się zapoznać z

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
	tworzenia kopii zapasowych.	instrukcjami.
Operacja tworzenia kopii zapasowej oczekuje	Alert jest generowany, gdy wystąpi konflikt harmonogramu i w tym samym czasie zostaną zainicjowane dwa zadania tworzenia kopii zapasowej. W takim przypadku drugie zadanie tworzenia kopii zapasowej jest umieszczane w kolejce, gdzie czeka do czasu zakończenia lub zatrzymania pierwszego zadania.	Dopilnuj, aby operacje tworzenia kopii zapasowych były uruchamiane w spodziewanych oknach czasowych i zgodnie z ich harmonogramem oraz zapobiegaj konfliktom w harmonogramie.
Operacja tworzenia kopii zapasowej nie odpowiada	Alert jest generowany, gdy operacja tworzenia kopii zapasowej od jakiegoś czasu nie sygnalizuje żadnego postępu i być może została zablokowana.	Przyczyną problemu może być zablokowanie. Więcej informacji można znaleźć w tym artykule bazy wiedzy Knowledge Base.
Operacja tworzenia kopii zapasowej nie rozpoczęła się	Alert jest generowany, gdy z jakiegoś nieznanego powodu zaplanowana operacja tworzenia kopii zapasowej nie została uruchomiona.	Upewnij się, że korzystasz z najnowszej wersji produktu Acronis Backup. • Jeśli komputer z agentem był dostępny w czasie rozpoczęcia tworzenia kopii zapasowej: 1. Edytuj czas rozpoczęcia zadania tworzenia kopii zapasowej. 2. Jeśli ten alert znów wystąpi, ponownie utwórz zadanie tworzenia kopii zapasowej. 3. Jeśli nowo utworzone zadanie tworzenia kopii zapasowej również wyzwala alert, zwróć się o pomoc do zespołu pomocy technicznej. • Jeśli agent był w trybie offline: 1. Nie wyłączaj komputera podczas operacji tworzenia kopii zapasowej. 2. Jeśli komputer nie został wyłączony, upewnij się, że usługa Acronis Managed Machine Service jest uruchomiona: Start ->

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
		Wyszukaj -> Services.msc -> znajdź usługę Acronis Managed Machine Service. Jeśli potrzebujesz pomocy, skontaktuj się z zespołem pomocy technicznej.
Nieznany status kopii zapasowej	Alert jest generowany, gdy o zaplanowanej godzinie tworzenia kopii zapasowej agent kopii zapasowych był w trybie offline. Dopóki agent nie przejdzie w tryb online, status kopii zapasowych zasobów będzie nieznany.	1. Sprawdź, czy agent może się znajdować w trybie offline (na przykład jest to notebook znajdujący się poza siecią serwera zarządzania). 2. Jeśli agent nie powinien być w trybie offline, upewnij się, że jest uruchomiona usługa Acronis Managed Machine Service: Start -> Wyszukaj -> services.msc -> znajdź usługę Acronis Managed Machine Service i sprawdź jej status. Jeśli usługa jest zatrzymana, uruchom ją.
Brak kopii zapasowej	Alert jest generowany, gdy operacja tworzenia kopii zapasowej się nie powiedzie przez więcej niż [dni od utworzenia ostatniej kopii zapasowej] dni.	
Kopia zapasowa jest uszkodzona	Alert jest generowany, gdy operacja sprawdzania poprawności zakończy się powodzeniem i wykaże, że kopia zapasowa jest uszkodzona.	Postępuj zgodnie z instrukcjami opisanymi w artykule Rozwiązywanie problemów z uszkodzonymi kopiami zapasowymi. Jeśli potrzebujesz pomocy w zidentyfikowaniu głównej przyczyny uszkodzenia archiwum, skontaktuj się z zespołem pomocy technicznej.
Niepowodzenie ciągłej ochrony danych	Alert jest generowany w przypadku niepowodzenia operacji tworzenia kopii zapasowej w ramach ciągłej ochrony.	Zweryfikuj następujące ograniczenia: 1. Ciągła ochrona danych jest obecnie obsługiwana tylko w przypadku systemu plików NTFS i następujących systemów operacyjnych: • Komputer stacjonarny: Windows 7 lub nowszy

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
		• Serwer: Windows Server 2008 R2 lub nowszy 2. Funkcja Ciągła ochrona danych nie obsługuje partycji **Acronis Secure Zone** jako miejsca docelowego. 3. Foldery NFS zamontowane w systemie Windows nie są obsługiwane. 4. Ciągła replikacja nie jest obsługiwana: jeśli w planie ochrony występują dwie lokalizacje, wycinki w ramach ciągłej ochrony danych są tworzone tylko w pierwszym miejscu docelowym, po czym zmiany są replikowane do drugiego miejsca przy następnej operacji tworzenia kopii zapasowej. 5. Jeśli zmiany w lokalnym folderze chronionym są stosowane ze źródła sieciowego (na przykład gdy użytkownicy uzyskują dostęp do folderu z sieci), funkcja Ciągła ochrona danych ich nie wykrywa. 6. W przypadku używania pliku, na przykład wprowadzania pewnych zmian w pliku programu Excel, funkcja Ciągła ochrona danych nie wykrywa tych zmian. Aby te zmiany były wykrywane przez funkcję Ciągła ochrona danych, należy je zapisać i zamknąć plik.
Konfiguracja hostów Hyper-V jest nieprawidłowa	Alert jest generowany, gdy na hostach Hyper-V o tej samej nazwie hosta są zainstalowane co najmniej dwa agenty dla Hyper-V, co nie jest obsługiwane na tym samym poziomie konta.	W celu uniknięcia konfliktów należy zarejestrować te agenty dla Hyper-V w różnych jednostkach podrzędnych tego konta.
Sprawdzenie poprawności nie powiodło się	Alert jest generowany, gdy proces sprawdzania poprawności kopii zapasowej	Sprawdź dziennik błędnej operacji: kliknij komputer, aby go zaznaczyć, kliknij **Działania**, a następnie znajdź

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
	nie może zostać ukończony.	ostrzeżenie w dzienniku. Komunikat powinien sygnalizować główną przyczynę problemu.
Nie można migrować kopii zapasowych w chmurze do nowego formatu	Alert jest generowany w przypadku niepowodzenia migracji kopii zapasowej w chmurze do nowego formatu.	Więcej informacji na temat migracji archiwów programu Acronis Cyber Backup Advanced można znaleźć w tym artykule bazy wiedzy Knowledge Base. Więcej informacji na temat migracji archiwów programu Acronis Cyber Backup można znaleźć w tym artykule bazy wiedzy Knowledge Base. Zanim skontaktujesz się z zespołem pomocy technicznej, użyj narzędzia migrate_archives, aby zebrać następujące raporty: **migrate_archives.exe --account=<Acronis Account> --password=<password> --subaccounts=All > raport1.txt** **migrate_archives.exe --cmd=finishUpgrade --account=<Acronis Account> --password=<password> > raport2.txt**
Brak hasła szyfrowania	Alert jest generowany, gdy klucz szyfrowania bazy danych jest nieprawidłowy bądź uszkodzony albo gdy go wcale nie ma.	W przypadku zgubienia lub zapomnienia hasła nie da się odzyskać zaszyfrowanych kopii zapasowych. Hasło lokalnie trzeba ustawić lokalnie — na chronionym urządzeniu. Nie można ustawić hasła szyfrowania w planie ochrony. Dodatkowe informacje można znaleźć w sekcji Ustawianie hasła szyfrowania.
Oczekiwanie na przesłanie	Alert jest generowany, jeśli w ramach zaplanowanej operacji sprawdzania zostanie wykryte, że w przypadku danego planu tworzenia kopii zapasowych archiwum funkcji Fizyczne dostarczanie danych do	

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
	chmury nie zostało przesłane do magazynu.	
Odzyskiwanie kopii zapasowej się nie powiodło	Alert jest generowany w przypadku niepowodzenia operacji odzyskiwania podczas próby odzyskania plików lub kopii zapasowych systemu.	Ustal dokładną datę niepowodzenia operacji tworzenia kopii zapasowej i spróbuj odzyskać dane z ostatniej udanej kopii zapasowej.

Alerty dotyczące odzyskiwania po awarii

Alert	Opis	Jak obsłużyć alert
Przekroczono limit miejsca	Alert jest generowany w przypadku przekroczenia elastycznego limitu Magazyn odzyskiwania po awarii.	Zwiększ limit lub usuń część kopii zapasowych z chmury.
Osiągnięto limit	Alert jest generowany w przypadku przekroczenia elastycznego limitu następujących pozycji oferty: • Serwer chmurowy. • Punkty obliczeniowe. • Publiczne adresy IP.	
Przekroczono limit miejsca	Alert jest generowany w przypadku przekroczenia sztywnego limitu Magazyn odzyskiwania po awarii. Ten magazyn jest używany przez serwery podstawowe i serwery odzyskiwania. W przypadku osiągnięcia nadwyżki tego limitu nie można tworzyć serwerów podstawowych i serwerów odzyskiwania ani dodawać/rozszerzać dysków istniejących serwerów podstawowych. W przypadku przekroczenia nadwyżki tego limitu nie można wykonywać przełączania awaryjnego ani uruchamiać zatrzymanego serwera. Działające serwery	

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
	kontynuują pracę.	
Przekroczono limit	Alert jest generowany w przypadku przekroczenia sztywnego limitu następujących pozycji oferty: • Serwery chmurowe. • Punkty obliczeniowe. • Publiczne adresy IP.	Rozważ zakup dodatkowych limitów lub wyłącz zadania tworzenia kopii zapasowych dla urządzeń, których już nie musisz chronić.
Błąd przełączania awaryjnego	Alert jest generowany, gdy po zainicjowaniu przełączania awaryjnego wystąpił problem z systemem.	1. Wybierz serwer odzyskiwania, a następnie kliknij **Edytuj**. 2. Zmniejsz zasoby procesora / pamięci RAM serwera odzyskiwania. 3. Spróbuj ponownie wykonać przełączanie awaryjne.
Błąd testowego przełączania awaryjnego	Alert jest generowany, gdy po zainicjowaniu testowego przełączania awaryjnego wystąpił problem z systemem.	1. Wybierz serwer odzyskiwania, a następnie kliknij **Edytuj**. 2. Zmniejsz zasoby procesora / pamięci RAM serwera odzyskiwania. 3. Spróbuj ponownie wykonać testowe przełączanie awaryjne. **Uwaga** Upewnij się, że adres IP w sieci produkcyjnej jest taki sam jak adres IP skonfigurowany na serwerze DHCP.
Błąd powrotu po awarii	Alert jest generowany, gdy po zainicjowaniu powrotu po awarii wystąpił problem z systemem.	Na liście magazynów kopii zapasowych jest widoczna błędna lokalizacja: ma numer zamiast nazwy (zwykle nazwa lokalizacji jest taka sama jak jedna z już istniejących nazw użytkownika) i nie została utworzona przez Ciebie. Usuń błędną lokalizację: 1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych**. 2. Znajdź lokalizację i kliknij ikonę krzyżyka (x), aby ją usunąć.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
		3. Potwierdź wybór, klikając **Usuń**. 4. Ponów próbę przeprowadzenia operacji przełączania awaryjnego.
Anulowano powrót po awarii	Alert jest generowany w przypadku anulowania powrotu po awarii przez użytkownika.	Ręcznie odrzuć alert z poziomu konsoli.
Błąd połączenia VPN	Alert jest generowany w przypadku błędu połączenia VPN z przyczyn niezwiązanych z czynnościami użytkownika. Raport o statusie z urządzenia VPN jest nieaktualny.	W przypadku napotkania problemu podczas wdrażania lub nawiązywania połączenia z urządzeniem Acronis VPN skontaktuj się z zespołem pomocy technicznej. W wiadomości e-mail podaj następujące informacje: • Zrzuty ekranu przedstawiające komunikaty o błędach (jeśli występują) • Zrzut ekranu z interfejsu CLI urządzenia Acronis VPN • Twoje centrum danych Acronis Backup Cloud i nazwa grupy.
(VPN jest nieosiągalna) Brama łączności jest nieosiągalna	Alert jest generowany, gdy usługa Disaster Recovery nie może nawiązać komunikacji z bramą łączności. Raport o statusie z bramy łączności jest nieaktualny.	W razie problemu z wdrożeniem lub podłączeniem urządzenia Acronis VPN skontaktuj się z zespołem pomocy technicznej. W wiadomości e-mail podaj następujące informacje: • Zrzuty ekranu przedstawiające komunikaty o błędach (jeśli występują) • Zrzut ekranu z interfejsu CLI urządzenia Acronis VPN • Twoje centrum danych Acronis Backup Cloud i nazwa grupy
Wymagana jest zmiana przypisania adresu IP związanego z odzyskiwaniem po awarii	Alert jest generowany, gdy urządzenie VPN wykryje zmiany w sieci.	Zmień przypisanie adresu IP. Dodatkowe informacje można znaleźć w sekcji Zmienianie przypisania adresów IP.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
Błąd bramy łączności	Alert jest generowany w przypadku niepowodzenia wdrożenia serwera VPN w chmurze.	Skorzystaj z narzędzia do weryfikacji połączenia i sprawdź jego dane wynikowe pod kątem błędów. Zezwól na oprogramowanie Acronis w sekcji ustawień kontroli aplikacji na zaporze i w oprogramowaniu antywirusowym.
Błąd tworzenia serwera podstawowego	Alert jest generowany, gdy serwer podstawowy nie został utworzony z powodu błędu.	
Błąd tworzenia serwera odzyskiwania	Alert jest generowany, gdy serwer odzyskiwania nie został utworzony z powodu błędu.	Upewnij się, że serwer odzyskiwania spełnia wymagania oprogramowania. Aby uzyskać więcej informacji, zobacz sekcję "Wymagania dotyczące oprogramowania" (s. 787).
Usunięcie serwera podstawowego	Alert jest generowany w przypadku usunięcia serwera podstawowego.	
Błąd odzyskiwania serwera	Alert jest generowany w przypadku niepowodzenia operacji odzyskiwania serwera podstawowego lub serwera odzyskiwania.	Znajdź szczegółowe informacje. Jeśli komunikat o błędzie jest ogólny lub niejasny (na przykład „Błąd wewnętrzny”), przejdź do sekcji **Odzyskiwanie po awarii → Serwery**, kliknięciem zaznacz komputer, którego dotyczy problem, i kliknij **Działania**. Kliknij działanie, a następnie kliknij to działanie lewym przyciskiem myszy, przytrzymując naciśnięty klawisz CTRL. Kliknij ikonę z wielokropkiem (...) działania, a następnie kliknij **Informacje o działaniach związanych z zadaniem**.
Utworzenie kopii zapasowej się nie powiodło	Alert jest generowany w przypadku niepowodzenia operacji tworzenia kopii zapasowej serwera chmurowego (podstawowego lub serwera w	1. Sprawdź połączenie z lokalizacją kopii zapasowych. 2. Sprawdź urządzenie z magazynem kopii zapasowych (lokalne kopie zapasowe).

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
	stanie przełączania awaryjnego w ramach środowiska produkcyjnego).	
Przekroczenie limitu sieci	Alert jest generowany w przypadku osiągnięcia maksymalnej liczby sieci w chmurze (5 sieci).	
Błąd runbooka	Alert jest generowany w przypadku niepowodzenia wykonania runbooka.	Sytuacja ta nie ma wpływu na funkcjonalność produktu i można alert bezpiecznie zignorować. Dodatkowe informacje można znaleźć w sekcji "Tworzenie runbooka" (s. 868).
Ostrzeżenie dotyczące runbooka	Alert jest generowany, gdy wykonywanie runbooka zostanie ukończone z ostrzeżeniami.	Sytuacja ta nie ma wpływu na funkcjonalność produktu i można alert bezpiecznie zignorować. Dodatkowe informacje można znaleźć w sekcji "Tworzenie runbooka" (s. 868).
Wymagana jest działanie użytkownika dotyczące runbooka	Alert jest generowany, gdy runbook oczekuje na działanie użytkownika.	Sytuacja ta nie ma wpływu na funkcjonalność produktu i można alert bezpiecznie zignorować. Dodatkowe informacje można znaleźć w sekcji "Tworzenie runbooka" (s. 868).
Zablokowano ruch internetowy	Alert jest generowany w przypadku zablokowania ruchu internetowego przez administratora.	
Odblokowano ruch internetowy	Alert jest generowany w przypadku odblokowania ruchu internetowego przez administratora.	
Nakładanie się sieci lokalnych	Alert jest generowany w przypadku wykrycia identycznych lub nakładających się sieci lokalnych.	
Za mały limit serwera dla przełącznika licencjonowania	Alert jest generowany w przypadku niewystarczającego limitu serwerów chmurowych.	• W przypadku wygenerowania alertu dotyczącego serwera fizycznego upewnij się, że

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
		dzierżawca i użytkownik mają wystarczający limit pozycji oferty **Serwery hostingowe** lub **Serwery**. • W przypadku wygenerowania alertu dotyczącego serwera wirtualnego upewnij się, że dzierżawca i użytkownik mają wystarczający limit pozycji oferty **Serwery hostingowe** lub **Maszyny wirtualne**. Serwer wirtualny nie może wykorzystywać limitu pozycji oferty **Serwery**.
Niewystarczająca pozycja oferty dla przełącznika licencjonowania	Alert jest generowany w przypadku wyłączenia pozycji oferty **Magazyn odzyskiwania po awarii**.	
Błąd przełącznika licencjonowania	Alert jest generowany w przypadku napotkania błędu podczas operacji uaktualniania funkcji odzyskiwania po awarii.	
Za mało punktów obliczeniowych dla przełącznika licencjonowania	Alert jest generowany w przypadku braku dostępnych punktów obliczeniowych.	Zwiększ sztywny limit pozycji oferty **Punkty obliczeniowe**.
Za mały limit pozycji oferty serwerów dla przełącznika licencjonowania	Alert jest generowany w przypadku wyłączenia pozycji oferty **Serwery chmurowe**.	
Zasady nie utworzyły serwera odzyskiwania	Alert jest generowany w przypadku błędu podczas konfigurowania infrastruktury odzyskiwania po awarii.	Ręcznie utwórz serwer odzyskiwania bez właściwości **Dostęp do Internetu**. Dodatkowe informacje można znaleźć w sekcji "Tworzenie serwera odzyskiwania" (s. 835).
Przełożono automatyczny test przełączania awaryjnego procesora operacji tworzenia kopii zapasowych	Alert jest generowany w przypadku przełożenia automatycznego testowego przełączania awaryjnego.	
Wyczerpano limit automatycznego testowego przełączania awaryjnego	Alert jest generowany w przypadku wygaśnięcia automatycznego testowego	

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
procesora operacji tworzenia kopii zapasowych	przełączania awaryjnego. **Uwaga** Podczas każdego automatycznego testowego przełączania awaryjnego wykorzystywane są punkty obliczeniowe.	
Ogólny błąd automatycznego testu przełączania awaryjnego procesora operacji tworzenia kopii zapasowych	Alert jest generowany, gdy nie udało się wykonać ostatniego zaplanowanego automatycznego testowego przełączania awaryjnego serwera odzyskiwania.	• Ręcznie uruchom testowe przełączanie awaryjne serwera odzyskiwania. Dodatkowe informacje można znaleźć w sekcji "Wykonywanie testowego przełączenia awaryjnego" (s. 839). • Poczekaj na następną zaplanowaną datę przeprowadzenia automatycznego przełączania awaryjnego.
Błąd operacji przesyłania danych w ramach powrotu po awarii	Alert jest generowany w przypadku niepowodzenia fazy przesyłania danych w ramach powrotu po awarii.	
Niepowodzenie powrotu po awarii	Alert jest generowany w przypadku błędu operacji powrotu po awarii.	Na liście magazynów kopii zapasowych jest widoczna błędna lokalizacja: ma numer zamiast nazwy (zwykle nazwa lokalizacji jest taka sama jak jedna z już istniejących nazw użytkownika) i nie została utworzona przez Ciebie. Usuń błędną lokalizację: 1. W oprogramowaniu Cyber Protection przejdź do sekcji **Magazyn kopii zapasowych**. 2. Znajdź lokalizację i kliknij ikonę krzyżyka (x), aby tę lokalizację usunąć. 3. Potwierdź wybór, klikając **Usuń**. 4. Rozpocznij ponownie przełączanie awaryjne.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
Niepowodzenie potwierdzenia powrotu po awarii	Alert jest generowany w przypadku niepowodzenia potwierdzenia powrotu po awarii.	
Komputer używany do powrotu po awarii jest gotowy do przełączenia	Alert jest generowany, gdy komputer jest gotowy do przełączenia.	
Ukończono przełączanie w ramach powrotu po awarii	Alert jest generowany po pomyślnym przełączeniu.	Ręcznie odrzuć alert z poziomu konsoli.
Agent w miejscu docelowym powrotu po awarii jest w trybie offline	Alert jest generowany, gdy agent jest w trybie offline.	

Alerty dotyczące ochrony przed złośliwym oprogramowaniem

Alert	Opis	Jak obsłużyć alert
Wykryto podejrzane działanie w ramach połączenia zdalnego	Alert jest generowany w przypadku wykrycia ransomware pochodzącego z połączenia zdalnego.	Ręcznie odrzuć alert z poziomu konsoli.
Wykryto podejrzane działanie	Alert jest generowany w przypadku wykrycia ransomware na maszynie.	Ręcznie odrzuć alert z poziomu konsoli. w celu dezaktywowania alertu. W zależności od opcji określonej w planie usługi Active Protection złośliwy proces zostaje zatrzymany, zmiany wprowadzone przez proces zostają cofnięte lub żadne czynności nie zostały jeszcze podjęte i należy rozwiązać problem ręcznie. Zapoznaj się ze szczegółami alertu, aby sprawdzić, który proces szyfruje pliki i których plików dotyczy problem. Jeśli ustalisz, że proces szyfrujący pliki jest uzasadniony (wystąpił fałszywy alarm), dodaj ten proces do sekcji Zaufane procesy: 1. Otwórz plan usługi Active Protection. 2. Kliknij **Edytuj**, aby zmodyfikować ustawienia. 3. W sekcji **Zaufane procesy** określ zaufane procesy, które nigdy nie będą

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
		uznawane za ransomware. Podaj pełną ścieżkę do wykonywalnego procesu, zaczynając od litery dysku. Na przykład: `C:\Windows\Temp\er76s7sdkh.exe`
Wykryto działanie związane z cryptominingiem	Alert jest generowany w przypadku wykrycia na maszynie niepożądanych programów do cryptominingu.	Ręcznie odrzuć alert z poziomu konsoli.
Obrona rekordu MBR: Wykryto podejrzane działanie i zawieszono operację	Alert jest generowany w przypadku wykrycia na maszynie oprogramowania ransomware (zwłaszcza jeśli ransomware zmodyfikuje partycję MBR/GPT).	Ręcznie odrzuć alert z poziomu konsoli.
Określono nieprawidłową ścieżkę sieciową	Alert jest generowany, gdy ścieżka odzyskiwania podana przez administratora nie jest ścieżką do folderu lokalnego.	Podaj ścieżkę lokalną na potrzeby ochrony folderu sieciowego (ścieżkę odzyskiwania). Ręcznie odrzuć alert z poziomu konsoli.
Proces krytyczny został dodany jako szkodliwy do planu usługi Active Protection	Alert jest generowany w przypadku dodania procesu krytycznego jako zablokowanego do listy wykluczeń z ochrony.	Ręcznie odrzuć alert z poziomu konsoli.
Nie udało się zastosować zasad usługi Active Protection	Alert jest generowany w przypadku niepowodzenia zastosowania zasad usługi Active Protection.	Przeczytaj komunikat o błędzie, aby się dowiedzieć, dlaczego nie można zastosować zasad usługi Active Protection.
Secure Zone: Wykryto i zablokowano nieautoryzowaną operację	Alert jest generowany w przypadku wykrycia na maszynie oprogramowania ransomware (zwłaszcza jeśli ransomware zmodyfikuje partycję ASZ).	Ręcznie odrzuć alert z poziomu konsoli.
Usługa Active Protection nie działa	Alert jest generowany w przypadku awarii lub niedziałania usługi Active Protection.	Przeczytaj komunikat o błędzie, aby się dowiedzieć, dlaczego usługa Active Protection nie działa.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
Usługa Active Protection jest niedostępna	Alert jest generowany, gdy usługa Active Protection jest niedostępna z powodu niekompatybilności lub braku sterownika.	Sprawdź dzienniki zdarzeń systemu Windows pod kątem awarii usługi Acronis Active Protection (acronis_protection_service.exe).
Konflikt z innym rozwiązaniem do ochrony bezpieczeństwa	Alert jest generowany, gdy usługa Active Protection jest niedostępna dla komputera „{{resourceName}}" z powodu wykrycia konfliktu z innym rozwiązaniem do ochrony bezpieczeństwa. Aby włączyć usługę Active Protection, należy wyłączyć lub odinstalować rozwiązanie powodujące konflikt.	**Rozwiązanie 1**. Jeśli chcesz użyć ochrony Acronis w czasie rzeczywistym, odinstaluj z maszyny oprogramowanie antywirusowe innej firmy. **Rozwiązanie 2**. Jeśli chcesz używać oprogramowania antywirusowego innej firmy, w planie ochrony stosowanym do maszyny wyłącz ochronę Acronis w czasie rzeczywistym, Filtrowanie adresów URL i program antywirusowy Windows Defender.
Niepowodzenie czynności dotyczącej kwarantanny	Alert jest generowany w sytuacji, gdy oprogramowanie antywirusowe nie poddało wykrytego złośliwego oprogramowania kwarantannie.	Przeczytaj komunikat o błędzie, aby się dowiedzieć, dlaczego nie udało się zastosować kwarantanny.
Wykrycie złośliwego procesu	Alert jest generowany, gdy mechanizm zachowań wykryje na maszynie złośliwe oprogramowanie (typ procesu). Wykryte złośliwe oprogramowanie zostaje poddane kwarantannie.	Ręcznie odrzuć alert z poziomu konsoli.
Wykrycie złośliwego procesu bez poddania go kwarantannie	Alert jest generowany, gdy mechanizm zachowań wykryje na maszynie złośliwe oprogramowanie (typ procesu). Wykryte złośliwe oprogramowanie nie zostaje poddane kwarantannie.	Ręcznie odrzuć alert z poziomu konsoli.
Wykryto i zablokowano złośliwe oprogramowanie	Alert jest generowany, gdy podczas zaplanowanego	Ręcznie odrzuć alert z poziomu konsoli.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
(ODS)	skanowania na maszynie zostanie wykryte złośliwe oprogramowanie. Wykryte złośliwe oprogramowanie zostaje poddane kwarantannie.	
Wykryto i zablokowano złośliwe oprogramowanie (RTP)	Alert jest generowany, gdy funkcja ochrony w czasie rzeczywistym wykryje na maszynie złośliwe oprogramowanie. Wykryte złośliwe oprogramowanie zostaje poddane kwarantannie.	Ręcznie odrzuć alert z poziomu konsoli.
Wykryto złośliwe oprogramowanie w kopii zapasowej	Alert jest generowany, gdy podczas skanowania kopii zapasowych na maszynie zostanie wykryte złośliwe oprogramowanie.	Ręcznie odrzuć alert z poziomu konsoli.
Wykryto konflikt między modułem Ochrona antywirusowa w czasie rzeczywistym a programem zabezpieczającym	Alert jest generowany w sytuacji, gdy oprogramowaniu antywirusowemu nie udało się zarejestrować w Centrum zabezpieczeń systemu Windows.	Wyłącz lub odinstaluj produkt zabezpieczający innej firmy albo wyłącz w planie ochrony ochronę przed złośliwym oprogramowaniem w czasie rzeczywistym.
Nie można uruchomić modułu Microsoft Security Essentials	Alert jest generowany w przypadku niepowodzenia uruchomienia modułu Microsoft Security Essentials.	Przeczytaj komunikat o błędzie, aby się dowiedzieć, dlaczego nie udało się uruchomić modułu Microsoft Security Essentials.
Ochrona w czasie rzeczywistym jest niedostępna, ponieważ jest zainstalowane oprogramowanie antywirusowe innej firmy	Alert jest generowany, gdy nie uda się włączyć ochrony w czasie rzeczywistym, ponieważ program antywirusowy innej firmy nadal ma włączoną ochronę w czasie rzeczywistym.	Wyłącz lub odinstaluj produkt zabezpieczający innej firmy albo wyłącz w planie ochrony ochronę przed złośliwym oprogramowaniem w czasie rzeczywistym.
Ochrona w czasie rzeczywistym jest niedostępna z powodu	Alert jest generowany, gdy ochrona w czasie rzeczywistym jest	Sprawdź komunikat o błędzie, aby zobaczyć, dlaczego nie powiodła się instalacja sterownika na maszynie.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
niekompatybilności lub braku sterownika	niedostępna z powodu niekompatybilności lub braku sterownika.	
Usługa Cyber Protection (lub Active Protection) nie odpowiada	Alert jest generowany, gdy usługa Ochrona cybernetyczna odpowie na sondę ping wysłaną z konsoli w celu kontroli kondycji.	Ręcznie odrzuć alert z poziomu konsoli.
Niepowodzenie aktualizacji definicji zabezpieczeń	Alert jest generowany w przypadku niepowodzenia aktualizacji definicji zabezpieczeń.	Przeczytaj komunikat o błędzie, aby się dowiedzieć, dlaczego nie udało się zaktualizować definicji zabezpieczeń.
Ochrona przed manipulacjami jest włączona	Alert jest generowany, gdy nie można zmienić ustawień usługi Microsoft Defender, ponieważ jest włączona ochrona przed manipulacjami.	Wyłącz ustawienia ochrony przed manipulacjami na obciążeniu z systemem Windows.
Niepowodzenie wykonania modułu Windows Defender	Alert jest generowany w przypadku niepowodzenia uruchomienia modułu Windows Defender.	Przeczytaj komunikat o błędzie, aby się dowiedzieć, dlaczego nie udało się uruchomić modułu Windows Defender.
Program Windows Defender został zablokowany przez oprogramowanie antywirusowe innej firmy	Alert jest generowany w przypadku zablokowania Windows Defender z powodu zainstalowania na komputerze programu antywirusowego innej firmy.	Wyłącz lub odinstaluj ten produkt zabezpieczający innej firmy.
Konflikt zasad grupy	Alert jest generowany, gdy nie można zmienić ustawień programu Microsoft Defender, ponieważ jest on kontrolowany przez zasady grupy.	Wyłącz ustawienia zasad grupy w maszynie z systemem Windows.
Program Microsoft Security Essentials podjął działanie mające na celu ochronienie komputera przed złośliwym oprogramowaniem	Alert jest generowany, gdy program Microsoft Security Essentials usunie złośliwe oprogramowanie lub podda je kwarantannie.	Ręcznie odrzuć alert z poziomu konsoli.
Program Microsoft Security	Alert jest generowany, gdy	Ręcznie odrzuć alert z poziomu konsoli.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
Essentials wykrył złośliwe oprogramowanie	program Microsoft Security Essentials wykryje złośliwe lub inne potencjalnie niepożądane oprogramowanie.	

Alerty dotyczące licencjonowania

Alert	Opis	Jak obsłużyć alert
Prawie osiągnięto limit miejsca	Alert jest generowany, gdy poziom wykorzystania spadnie poniżej 80% (po oczyszczeniu lub uaktualnieniu limitu).	Rozważ zakup dodatkowej pamięci masowej lub zwolnienie miejsca w chmurze.
Przekroczono limit miejsca	Alert jest generowany, gdy zostanie wykorzystane 100% limitu miejsca.	Kup więcej miejsca w pamięci masowej. Dodatkowe informacje można znaleźć w tym artykule bazy wiedzy Knowledge Base.
Osiągnięcie limitu obciążenia	Alert jest generowany, gdy wykorzystanie pozycji oferty > 0 i użycie > limit, ale użycie <= limit + nadwyżka.	
Przekroczenie limitu obciążenia	Alert jest generowany, gdy wykorzystanie pozycji oferty > limit + nadwyżka.	
Obciążenie nie ma limitu, aby zastosować plan tworzenia kopii zapasowych (zasób nie ma limitu usługi)	Alert jest generowany, gdy: • Limit został ręcznie usunięty: **Urządzenie** > **Szczegóły** > **Limit usług**, a następnie kliknij **Zmień** i wybierz **Brak limitu**. • Wyłączono pozycję oferty **Konsola zarządzania**. • Wartość limit+nadwyżka pozycji oferty **Konsola zarządzania** została zmniejszona do poziomu poniżej bieżącego wykorzystania.	
Nie można chronić obciążenia przy użyciu przypisanego limitu	Alert jest generowany w przypadku zbyt małej pozycji oferty i trzeba mieć: • grupę dynamiczną,	

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
	• plan tworzenia kopii zapasowych przypisany do tej grupy. • zasób, który należy do tej grupy dynamicznej, ale ma on pewne cechy, które uniemożliwiają zastosowanie do niego tego samego planu tworzenia kopii zapasowych.	
Licencja subskrypcyjna wygasła	Alert jest generowany w przypadku wygaśnięcia licencji.	Po wygaśnięciu subskrypcji wszystkie funkcje produktu — z wyjątkiem odzyskiwania — zostają zablokowane do czasu kolejnego odnowienia subskrypcji. Dane uwzględnione w kopii zapasowej nadal są dostępne do odzyskania. Kup nową licencję. **Uwaga** Jeśli masz niedawno wykupioną nową subskrypcję, ale nadal otrzymujesz komunikat, że subskrypcja wygasła, zaimportuj nową subskrypcję z konta Acronis Konto: w konsoli zarządzania przejdź do sekcji **Ustawienia** -> **Licencje** , a następnie w prawym górnym rogu kliknij **Synchronizuj**. Subskrypcje zostaną zsynchronizowane.
Licencja subskrypcyjna wkrótce wygaśnie	Alert jest generowany, jeśli licencja wygaśnie za mniej niż 30 dni.	Kup nową subskrypcję.

Alerty dotyczące modułu Filtrowanie adresów URL

Alert	Opis	Jak obsłużyć alert
Zablokowano złośliwy adres URL	Alert jest generowany, gdy funkcja Filtrowanie adresów URL zablokuje złośliwy adres URL.	Sprawdź ustawienia funkcji Filtrowanie adresów URL. Funkcja Filtrowanie adresów URL blokuje strony, które powinny być blokowane zgodnie z ustawieniami

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
		określonymi w sekcji Filtrowanie adresów URL. Dodatkowe informacje można znaleźć w sekcji "Filtrowanie adresów URL" (s. 906).
Zignorowano ostrzeżenie o złośliwym adresie URL	Alert jest generowany w przypadku wybrania opcji kontynuowania przy użyciu złośliwego adresu URL zablokowanego przez funkcję Filtrowanie adresów URL.	Sprawdź ustawienia funkcji Filtrowanie adresów URL.
Wykryto konflikt między modułem Filtrowanie adresów URL a programem zabezpieczającym	Alert jest generowany, gdy funkcja Filtrowanie adresów URL nie może zostać włączona z powodu konfliktu z innym produktem zabezpieczającym.	Sprawdź ustawienia funkcji Filtrowanie adresów URL.
Zablokowano adres URL witryny internetowej	Alert jest generowany, gdy adres URL spełnia wszystkie kryteria określone w zablokowanej kategorii w ramach funkcji Filtrowanie adresów URL.	Sprawdź ustawienia funkcji Filtrowanie adresów URL.

Alerty dotyczące modułu EDR

Alert	Opis	Jak obsłużyć alert
Wykryto incydent	Alert jest generowany, gdy zostanie utworzony incydent lub zostanie zaktualizowany status już istniejącego incydentu.	Alert ten stanowi informację o nowym incydencie lub o aktualizacji starego incydentu. Można wyświetlić alert i go zamknąć. Można otworzyć incydent w celu dokładniejszego zbadania.
Wykryto wskaźnik naruszenia zabezpieczeń (indicator of compromise, IOC)	Alert jest generowany, gdy usługa wyszukiwania zagrożeń EDR IOC wykryje nowy wskaźnik naruszenia zabezpieczeń.	Ten alert ma za zadanie poinformować o wykryciu wskaźnika IOC na jednym lub wielu obciążeniach. Po wyświetleniu alertu można kliknąć zawarte w nim łącze, aby wyświetlić szczegóły wskaźnika IOC.
Nie można izolować obciążenia od sieci	Alert jest generowany, gdy użytkownik wyzwoli czynność	Podejmij konieczne kroki.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
	odizolowania komputera od sieci i czynność ta się nie powiedzie.	
Nie można ponownie połączyć obciążenia z siecią	Alert jest generowany, gdy użytkownik wyzwoli czynność wznowienia połączenia komputera z siecią i czynność ta się nie powiedzie.	Podejmij konieczne kroki.
Zmodyfikowano ustawienia zapory Windows Defender	Alert jest generowany, gdy na izolowanym komputerze zmodyfikowano ustawienia zapory.	Alert ten stanowi informację, że na izolowanym komputerze zmodyfikowano ustawienia zapory. Ma on charakter wyłącznie informacyjny i po jego wyświetleniu można go zamknąć.

Alerty związane z kontrolą urządzeń

Alert	Opis	Jak obsłużyć alert
Usługi kontroli urządzeń i zapobiegania utracie danych będą działać z ograniczoną liczbą funkcji (wykryto niekompatybilny procesor)	Alert jest generowany w przypadku uruchomienia agenta DeviceLock na komputerze fizycznym z procesorem obsługującym technologię CET.	Wyłącz tę opcję na komputerach, których dotyczy problem, aby uniknąć alertów.
Funkcja kontroli urządzeń nie jest jeszcze obsługiwana w systemie macOS Ventura	Alert jest generowany, gdy agent DeviceLock zostanie uruchomiony na komputerze fizycznym z systemem macOS Ventura i do agenta zostanie zastosowany plan ochrony z funkcją kontroli urządzeń. Dotyczy tylko wersji, w których występuje problem z paniką jądra powodowaną przez sterownik DeviceLock.	
Zezwolenie na przesłanie danych wrażliwych	Alert jest generowany, jeśli zostanie udzielone zezwolenie na przesłanie zawartości wrażliwej.	
Uzasadnione przesłanie danych wrażliwych	Alert jest generowany w przypadku uzasadnienia przesłania zawartości wrażliwej.	
Odmowa przesłania danych wrażliwych	Alert jest generowany, jeśli zostanie zablokowane przesłanie	

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
	zawartości wrażliwej.	
Przejrzyj wyniki uzyskane w trybie monitorowania Zapobieganie utracie danych	Alert jest generowany, gdy przychodzi czas na sprawdzenie wyników działania trybu Obserwacja: • Nie zastosowano licencji pakietu Advanced DLP. • Minął miesiąc od włączenia trybu Obserwacja w dowolnym planie ochrony zastosowanym do co najmniej jednej maszyny. • Minął miesiąc od wygenerowania ostatniego podobnego alertu i wykryto pewne wykorzystanie funkcji DLP w trybie Obserwacja.	
Zmieniono identyfikator zabezpieczeń dla użytkownika	Alert jest generowany w przypadku aktualizacji identyfikatora SID znanej nazwy użytkownika. Może się to zdarzyć, gdy system operacyjny zostanie ponownie zainstalowany na maszynie niedomenowej.	
Zablokowano dostęp do urządzeń peryferyjnych	Alert jest generowany, gdy zostaną zablokowane niektóre czynności (operacje odczytu/zapisu) w odniesieniu do obsługiwanych urządzeń.	
Nie można nawiązać połączenia ze zdalnym zasobem SSL.	Alert jest generowany, jeśli dostęp do zdalnego zasobu SSL jest blokowany z powodu dodatkowego mechanizmu zapobiegania uzgadnianiu zastosowanemu w zasobie.	Dodaj zasób do listy dozwolonych hostów zdalnych.

Alerty dotyczące systemu

Alert	Opis	Jak obsłużyć alert
Agent jest przestarzały	Alert jest generowany w przypadku przestarzałej wersji agenta.	Przejdź do listy agentów i zaktualizuj agenta.

© Acronis International GmbH, 2003-2024

Alert	Opis	Jak obsłużyć alert
Niepowodzenie aktualizacji automatycznej	Alert jest generowany w przypadku niepowodzenia automatycznej aktualizacji agenta.	Spróbuj przeprowadzić aktualizację ręcznie.
Po zainstalowaniu nowego agenta trzeba uruchomić ponownie urządzenie	Alert jest generowany, gdy po pomyślnej instalacji zdalnej wymagane jest ponowne uruchomienie.	Uruchom ponownie obciążenie.
Działanie nie powiodło się	Alert jest generowany w przypadku niepowodzenia jakiegoś działania.	Uruchom ponownie wszystkie usługi Acronis na maszynie.
Działanie zostało wykonane z ostrzeżeniami	Alert jest generowany, gdy działanie zostało ukończone pomyślnie, ale zostały wygenerowane pewne ostrzeżenia.	
Działanie nie odpowiada	Alert jest generowany, gdy nie odpowiada proces działania w toku.	
Nie można zaplanować wdrożenia	Alert jest generowany w przypadku niepowodzenia wdrożenia planu ochrony.	
Nie można przekonwertować nazwy użytkownika na identyfikator SID	Alert jest generowany w przypadku niepowodzenia konwersji identyfikatora SID harmonogramu.	

Widżety alertów

W sekcji widżetów alertów są widoczne następujące szczegóły alertów związanych z obciążeniem:

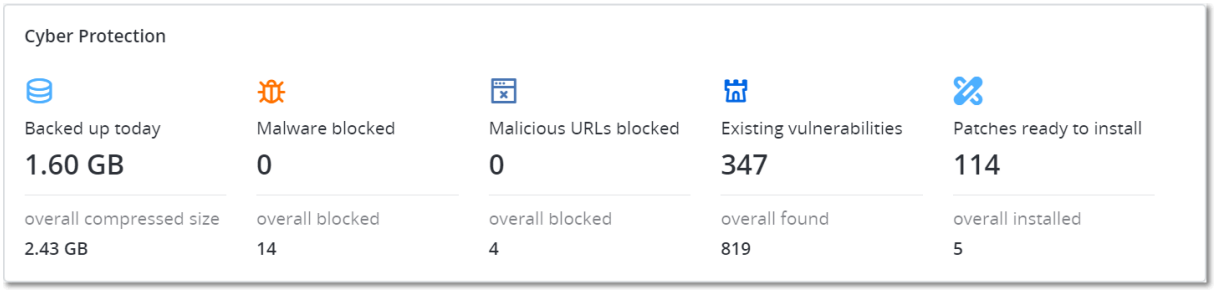
Pole	Opis
5 ostatnich alertów	Lista pięciu ostatnich alertów.
Historyczne zestawienie alertów	Widżet graficzny przedstawiający alerty według ich istotności, typu i zakresu czasu.
Podsumowanie aktywnych alertów	Widżet graficzny przedstawiający aktywne alerty według ich istotności i typu, a także łączną liczbę aktywnych alertów.
Historia alertów	Widok tabeli z alertami historycznymi.

© Acronis International GmbH, 2003-2024

Pole	Opis
Szczegóły aktywnych alertów	Widok tabeli z aktywnymi alertami.

Cyber Protection

Ten widżet przedstawia ogólne informacje o rozmiarze kopii zapasowych, zablokowanym złośliwym oprogramowaniu, zablokowanych adresach URL, znalezionych lukach w zabezpieczeniach i zainstalowanych poprawkach.



W górnym wierszu znajdują się bieżące dane statystyczne:

- **Uwzględnione w kopii zapasowej dzisiaj** — suma rozmiarów punktów odzyskiwania z ostatnich 24 godzin
- **Zablokowane złośliwe oprogramowanie** — liczba obecnie aktywnych alertów dotyczących zablokowanego złośliwego oprogramowania
- **Zablokowane adresy URL** — liczba obecnie aktywnych alertów dotyczących zablokowanych adresów URL
- **Występujące luki w zabezpieczeniach** — liczba obecnie występujących luk w zabezpieczeniach
- **Poprawki gotowe do instalacji** — liczba aktualnie dostępnych poprawek do zainstalowania

W dolnym wierszu znajdują się statystyki ogólne:

- Rozmiar wszystkich kopii zapasowych po kompresji
- Łączna liczba zablokowanych złośliwych programów na wszystkich komputerach
- Łączna liczba zablokowanych adresów URL na wszystkich komputerach
- Łączna liczba wykrytych luk w zabezpieczeniach na wszystkich komputerach
- Łączna liczba zainstalowanych aktualizacji/poprawek na wszystkich komputerach

Status ochrony

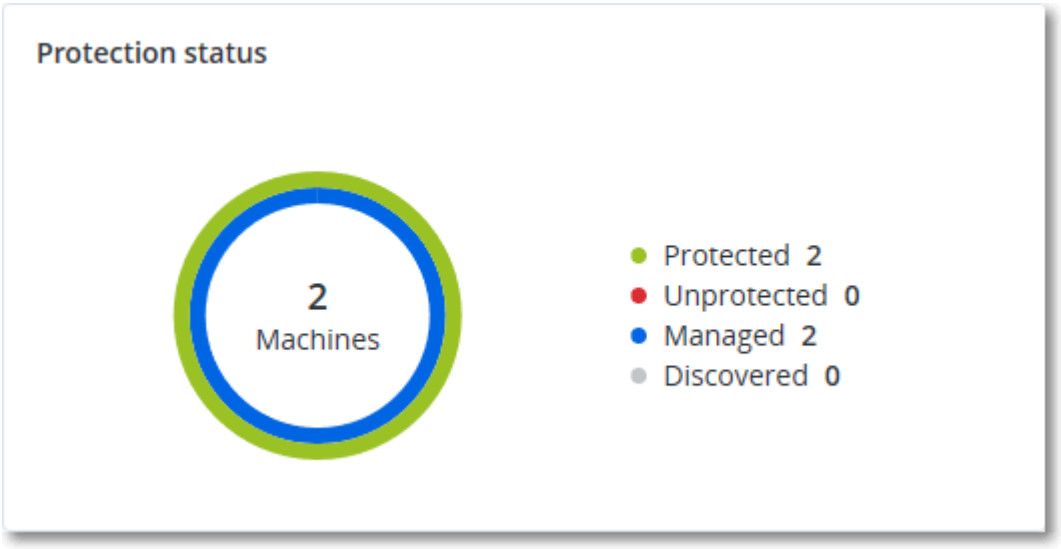
Ten widżet umożliwia wyświetlenie aktualnego statusu ochrony wszystkich komputerów.

Komputer może mieć jeden z następujących statusów:

© Acronis International GmbH, 2003-2024

- **Chronione** — komputery z zastosowanym planem ochrony.
- **Niechronione** — komputery bez zastosowanego planu ochrony. Są to zarówno wykryte, jak i zarządzane komputery, do których nie zastosowano planu ochrony.
- **Zarządzane** — komputery z zainstalowanym agentem ochrony.
- **Wykryto** — komputery bez zainstalowanego agenta ochrony.

Kliknięcie statusu komputera spowoduje przejście do listy komputerów o danym statusie, gdzie można znaleźć dodatkowe informacje.



Wykryte komputery

Ten widżet przedstawia listę komputerów wykrytych we wskazanym okresie.

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

© Acronis International GmbH, 2003-2024

Widżety pakietu Endpoint Detection and Response (EDR)

Moduł Endpoint Detection and Response (EDR) zawiera siedem widżetów. Wszystkie one są dostępne z poziomu pulpitu nawigacyjnego **Przegląd**. Trzy z tych widżetów są też domyślnie wyświetlane w ramach modułu EDR (zobacz "Przeglądanie incydentów" (s. 964)).

Oto te siedem dostępnych widżetów:

- Podział najliczniejszych incydentów według obciążeń
- Status zagrożeń (wyświetlany w module EDR)
- Historia ważności incydentów (wyświetlany w module EDR)
- Średni czas rozwiązywania problemu incydentu bezpieczeństwa
- Wykres spalania dotyczący incydentów bezpieczeństwa
- Wykrywanie na podstawie taktyk (wyświetlany w module EDR)
- Status sieciowy obciążeń

Podział najliczniejszych incydentów według obciążeń

Ten widżet przedstawia pięć obciążeń z największą liczbą incydentów (kliknij **Pokaż wszystko**, aby przejść do listy incydentów przefiltrowanej zgodnie z ustawieniami widżetu).

Zatrzymaj wskaźnik myszy na wierszu z obciążeniem, aby wyświetlić podział bieżącego stanu dochodzenia poszczególnych incydentów. Stany dochodzenia to **Nie uruchomiono**, **Trwa dochodzenie**, **Zamknięto** i **Fałszywe zgłoszenie**. Następnie kliknij obciążenie, które chcesz poddać dokładniejszym analizom. Lista incydentów jest odświeżana zgodnie z ustawieniami widżetu.

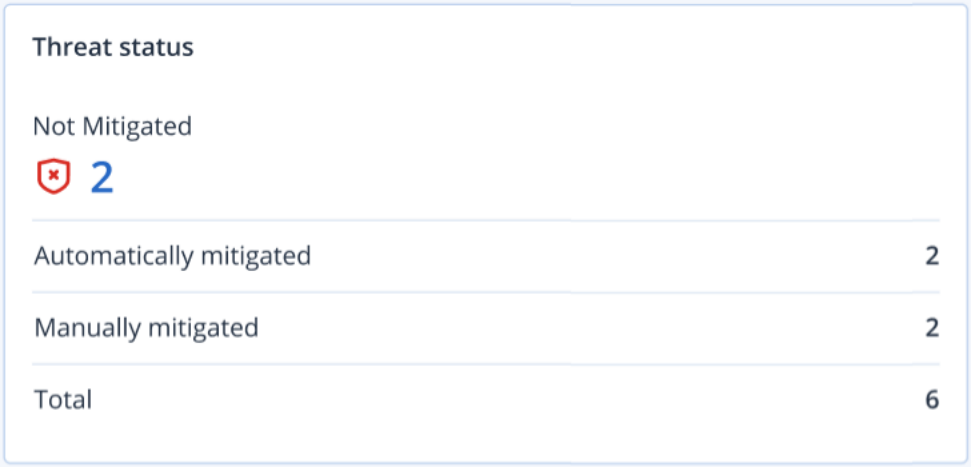
Status zagrożeń

Ten widżet przedstawia aktualny status zagrożeń w przypadku wszystkich obciążeń, z wyraźnym zaznaczeniem bieżącej liczby incydentów, których skutki nie zostały zniwelowane i które wymagają

© Acronis International GmbH, 2003-2024

dochodzenia. Widżet wskazuje również liczbę incydentów, których skutki zostały zniwelowane (ręcznie i/lub automatycznie przez system).

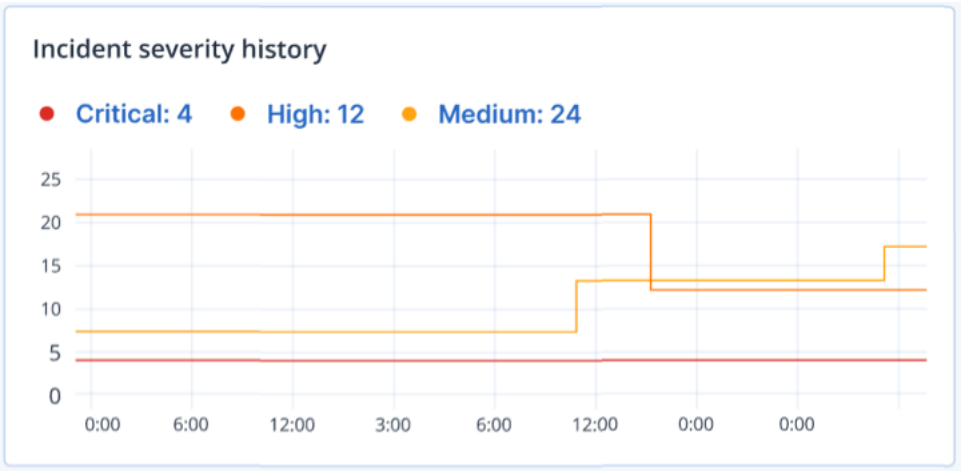
Kliknij liczbę z oznaczeniem **Nie zniwelowano** w celu wyświetlenia listy incydentów przefiltrowanej tak, aby były widoczne incydenty, których skutków nie zniwelowano.



Historia ważności incydentów

Ten widżet przedstawia ewolucję ataków z uwzględnieniem ich ważności, a także wspomaga sygnalizowanie kampanii ataków. Widoczne skoki oznaczają, że organizacja może być właśnie atakowana.

Wskaż wykres myszą, aby wyświetlić rozkład historii incydentów w określonym punkcie w ciągu ostatnich 24 godzin (jest to okres domyślny). Kliknij poziom ważności (**Krytyczne**, **Wysoki** lub **Średni**), jeśli chcesz wyświetlić listę odpowiednich incydentów. Nastąpi przekierowanie do listy incydentów przefiltrowanej tak, aby były na niej widoczne tylko incydenty odpowiadające wybranemu poziomowi ważności.

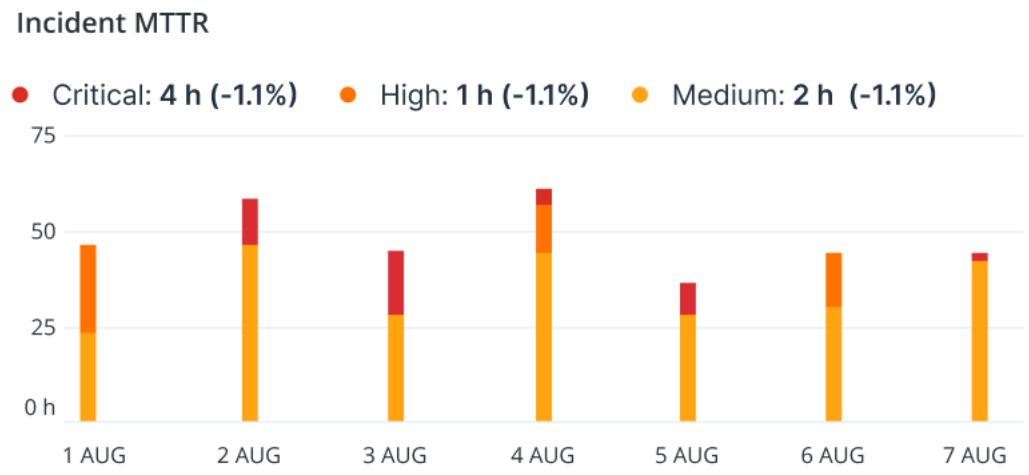


© Acronis International GmbH, 2003-2024

Średni czas rozwiązywania problemu incydentu bezpieczeństwa

Na tym widżecie jest przedstawiany średni czas rozwiązywania problemu związanego z incydentem bezpieczeństwa. Wskazuje on, jak szybko problemy incydentów są badane w ramach dochodzenia i rozwiązywane.

Kliknij kolumnę, aby wyświetlić podział incydentów według ich ważności (**Krytyczne**, **Wysoki** i **Średni**) oraz wskazanie, ile czasu zajęło rozwiązanie problemu o różnym poziomie ważności. Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem.



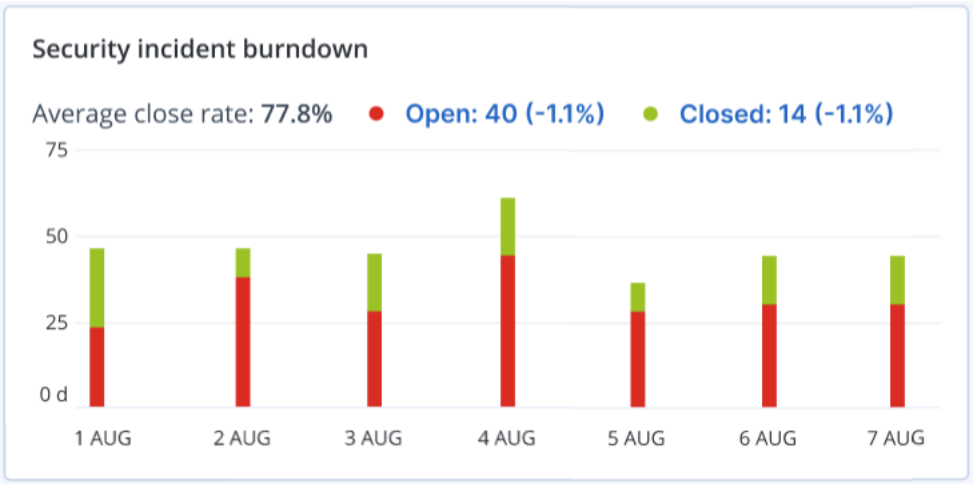
Wykres spalania dotyczący incydentów bezpieczeństwa

Ten widżet przedstawia wskaźnik efektywności zamykania incydentów. Liczba otwartych incydentów jest ujmowana w stosunku do liczby zamkniętych incydentów w danym okresie.

Zatrzymaj wskaźnik myszy na dowolnej kolumnie, aby wyświetlić podział zamkniętych i otwartych incydentów z wybranego dnia. Kliknięcie wartości Otwórz powoduje wyświetlenie listy incydentów przefiltrowanej tak, aby były wyświetlane tylko aktualnie otwarte incydenty (są w stanie **Trwa dochodzenie** lub **Nie uruchomiono**). Jeśli klikniesz wartość Zamknięto, zostanie wyświetlona lista incydentów przefiltrowana tak, aby były wyświetlane tylko incydenty, które nie są już otwarte (są w stanie **Zamknięto** lub **Fałszywe zgłoszenie**).

Wartość % podana w nawiasie oznacza wzrost lub spadek w porównaniu z poprzednim okresem.

© Acronis International GmbH, 2003-2024



Wykrywanie na podstawie taktyk

Na tym widżecie wyświetlana jest liczba przypadków wykrycia określonych technik ataku w ramach incydentów z wybranego okresu.

Wartości w kolorze zielonym i czerwonym wskazują, czy nastąpił wzrost, czy spadek w stosunku do poprzedniego okresu. W poniższym przykładzie odnotowano wzrost liczby ataków typu Eskalacja uprawnień oraz Command and Control w porównaniu z poprzednim okresem — może to sygnalizować konieczność analizy zarządzania poświadczeniami i wzmocnienia zabezpieczeń.

Detection by tactics

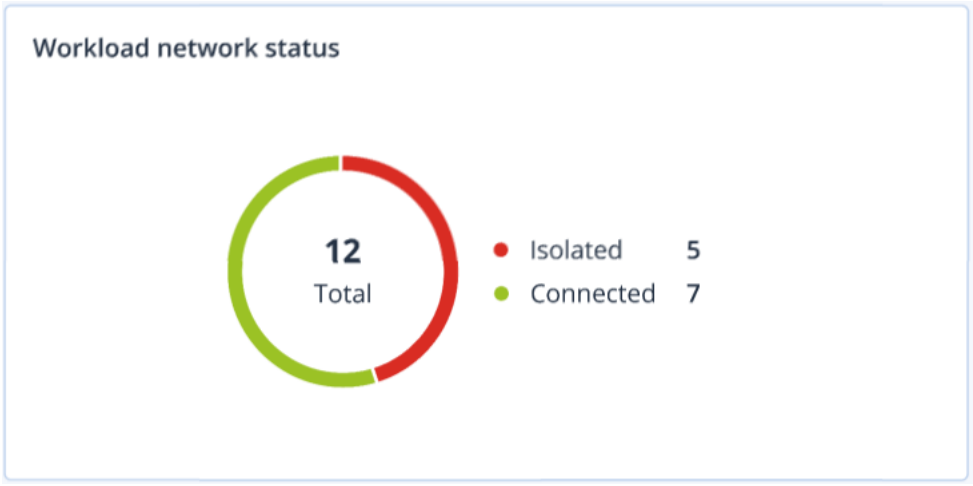
Initial Access	3	Discovery	3
Execution	7	Lateral Movement	0
Persistence	15	Collection	15
Priviledge Escalation	31	Command and Control	31
Defense Evasion	23	Exfiltration	23
Credential Access	7	Discovery	0
Impact	0	Resouce Development	0

Status sieciowy obciążeń

Ten widżet przedstawia bieżący status sieciowy obciążeń oraz wskazuje, ile obciążeń jest odizolowanych i ile połączonych.

Kliknij wartość Izolowano, aby wyświetlić listę Obciążenia z agentami (w menu **Obciążenia** w konsoli Cyber Protect) przefiltrowaną tak, aby były na niej widoczne tylko odizolowane obciążenia. Kliknij wartość Podłączono, aby wyświetlić listę obciążeń z agentami przefiltrowaną tak, aby były na nie wyświetlane tylko połączone obciążenia.

© Acronis International GmbH, 2003-2024



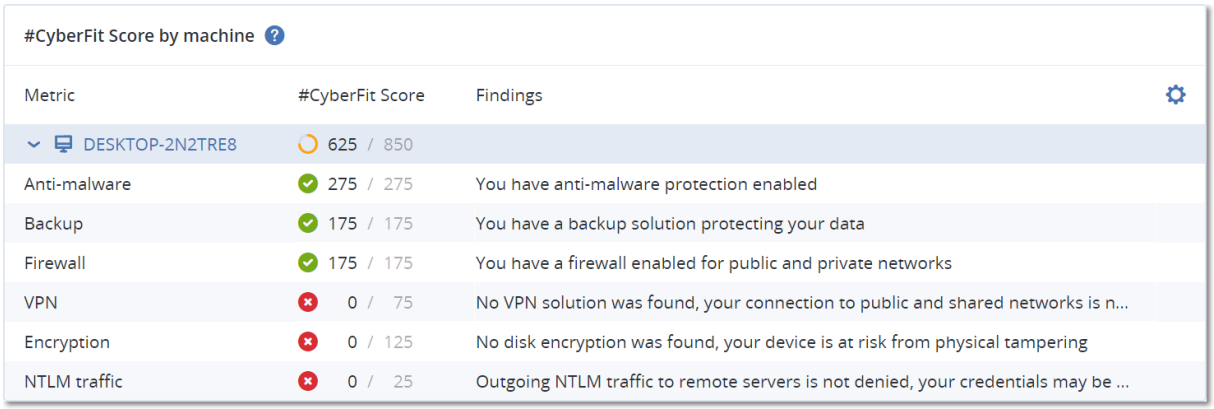
Wynik #CyberFit według komputerów

W przypadku tego widżetu jest pokazywany łączny wynik #CyberFit, jego wyniki składowe oraz diagnozy z badań poszczególnych wskaźników:

- Ochrona antywirusowa
- Kopia zapasowa
- Zapora
- VPN
- Szyfrowanie
- Ruch NTLM

Aby poprawić wartości poszczególnych wskaźników, zapoznaj się z zaleceniami przedstawionymi w raporcie.

Więcej informacji na temat wyniku #CyberFit można znaleźć w sekcji „Wyniki #CyberFit komputerów".



© Acronis International GmbH, 2003-2024

Monitorowanie kondycji dysków

Monitorowanie kondycji dysków dostarcza informacji o bieżącej kondycji dysku i prognozach na jej temat, dzięki czemu można zapobiec utracie danych, do której mogłoby dojść wskutek awarii dysku. Obsługiwane są zarówno dyski HDD, jak i dyski SSD.

Ograniczenia

- Prognoza kondycji dysków jest obsługiwana tylko w przypadku komputerów z systemem Windows.
- Monitorowane są tylko dyski komputerów fizycznych. Dyski maszyn wirtualnych nie mogą być monitorowane ani pokazywane na widżetach kondycji dysków.
- Konfiguracje macierzy RAID nie są obsługiwane. Widżety kondycji dysków nie zawierają żadnych informacji o komputerach z implementacją macierzy RAID.
- Dyski NVMe SSD nie są obsługiwane.

Kondycja dysku może być odzwierciedlana przez jeden z następujących statusów:

- **OK**
  Kondycja dysku w zakresie 70–100%.
- **Ostrzeżenie**
  Kondycja dysku w zakresie 30–70%.
- **Krytyczne**
  Kondycja dysku w zakresie 0–30%.
- **Obliczanie danych dysku**
  Trwa obliczanie aktualnego statusu dysku i generowanie prognozy.

Sposób działania

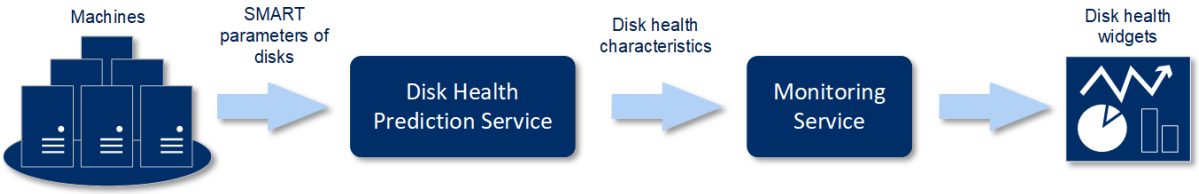
Usługa Prognoza kondycji dysków korzysta z modelu predykcyjnego opartego na sztucznej inteligencji.

1. Agent ochrony zbiera parametry SMART dysków i przekazuje te dane do usługi Prognoza kondycji dysków:
   - SMART 5 — liczba ponownie alokowanych sektorów.
   - SMART 9 — liczba godzin w stanie zasilania.
   - SMART 187 — zgłoszone nienaprawialne błędy.
   - SMART 188 — przekroczony limit czasu wykonywania polecenia.
   - SMART 197 — liczba oczekujących sektorów.
   - SMART 198 — liczba nienaprawialnych sektorów w trybie offline.
   - SMART 200 — wskaźnik błędów zapisu.

© Acronis International GmbH, 2003-2024

2. Usługa Prognoza kondycji dysków przetwarza uzyskane parametry SMART, sporządza prognozy i udostępnia następujące charakterystyki kondycji dysków:
   - Bieżący stan dysku: OK, Ostrzeżenie, Krytyczne.
   - Prognoza kondycji dysków: negatywna, stabilna, pozytywna.
   - Prawdopodobieństwo prognozy kondycji dysku w procentach.

   Prognoza obejmuje okres najbliższego miesiąca.
3. Usługa monitorowania odbiera te właściwości, a następnie wyświetla odpowiednie informacje na widżetach kondycji dysków w konsoli Cyber Protect.



Widżety kondycji dysków

Wyniki monitorowania kondycji dysków są prezentowane na następujących widżetach dostępnych w konsoli Cyber Protect.

- **Przegląd kondycji dysków** — widżet w formie mapy drzewa obejmującej dwa poziomy szczegółów, które można zmieniać przez pogłębianie analizy.
  - Poziom komputera
    Zawiera podsumowanie statusów kondycji dysków wybranych komputerów klientów. Widoczny jest tylko najbardziej krytyczny status dysku. Pozostałe statusy są pokazywane na etykietce wyświetlanej po wskazaniu danego bloku myszą. Rozmiar bloku komputera zależy od łącznego rozmiaru dysków tego komputera. Kolor bloku komputera zależy od najbardziej krytycznego wykrytego statusu dysku.

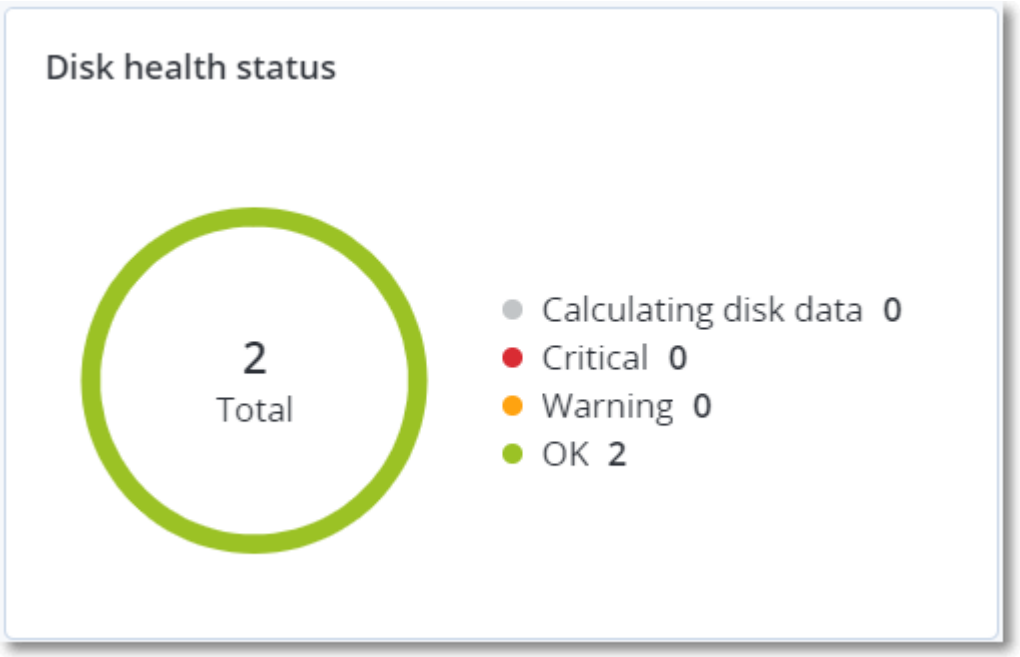
© Acronis International GmbH, 2003-2024

- Poziom dysku
  Zawiera aktualne statusy kondycji wszystkich dysków wybranego komputera. Każdy blok dysków zawiera jedną z następujących prognoz kondycji dysków wraz z jej prawdopodobieństwem wyrażonym w procentach:
  - Ulegnie pogorszeniu
  - Pozostanie stabilne

© Acronis International GmbH, 2003-2024

- Ulegnie poprawie

- **Status kondycji dysków** — widżet w postaci wykresu kołowego przedstawiający liczby dysków według poszczególnych statusów.



© Acronis International GmbH, 2003-2024

Alerty dotyczące statusów kondycji dysków

Kondycja dysku jest sprawdzana co 30 minut, a raz dziennie jest generowany odpowiedni alert. Gdy kondycja dysku zmieni się z **Ostrzeżenie** na **Krytyczne**, zawsze zostanie wygenerowany alert.

Nazwa alertu	Ważność	Status kondycji dysków	Opis
Możliwość awarii dysku	Ostrzeżenie	(30 – 70)	Dysk <nazwa dysku> komputera prawdopodobnie ulegnie awarii. Jak najszybciej utwórz pełną kopię zapasową obrazu dysku, wymień go, a następnie odzyskaj obraz na nowy dysk.
Bliska awaria dysku	Krytyczne	(0 – 30)	Dysk <nazwa dysku> komputera jest w stanie krytycznym i najprawdopodobniej bardzo szybko ulegnie awarii. Odradzamy tworzenie kopii zapasowej obrazu tego dysku, ponieważ dodatkowe obciążenie może spowodować jego awarię. Niezwłocznie utwórz kopię zapasową wszystkich najważniejszych plików z tego dysku i go wymień.

Mapa ochrony danych

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Funkcja mapy ochrony danych pozwala na wykrycie wszystkich ważnych danych i uzyskanie szczegółowych informacji o liczbie, rozmiarze, lokalizacji, statusach ochrony wszystkich ważnych plików w skalowalnym widoku mapy drzewa.

Każdy rozmiar bloku zależy od łącznej liczby lub łącznego rozmiaru wszystkich ważnych plików klienta bądź komputera.

Pliki mogą mieć jeden z następujących statusów ochrony:

- **Krytyczne** — 51–100% niechronionych plików z podanymi rozszerzeniami, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.
- **Niski** — 21–50% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.
- **Średni** — 1–20% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy

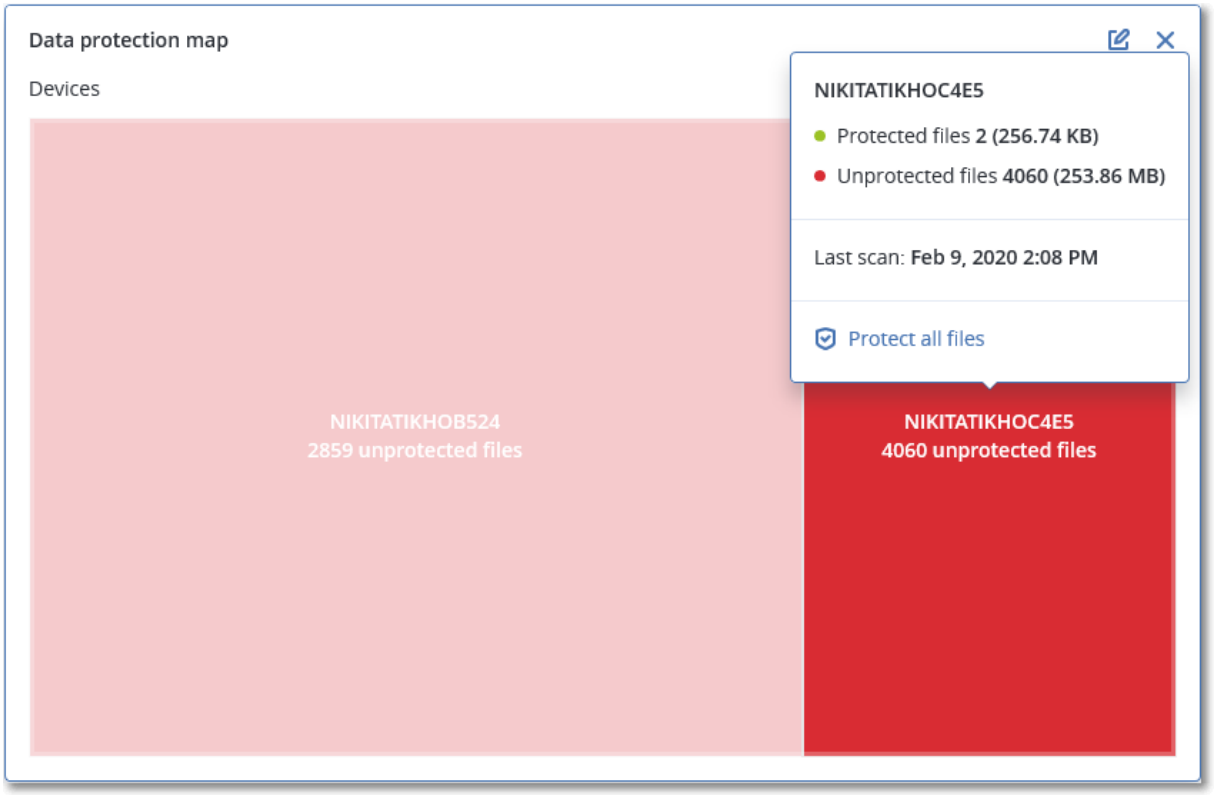
© Acronis International GmbH, 2003-2024

obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.

- **Wysoki** — wszystkie pliki z podanymi rozszerzeniami są chronione (uwzględniane w kopiach zapasowych) w przypadku wybranego komputera lub wybranej lokalizacji.

Wyniki kontroli ochrony danych można znaleźć na pulpicie nawigacyjnym monitorowania w widżecie Mapa ochrony danych — jest to mapa drzewa ze szczegółowymi informacjami na poziomie komputera:

- Poziom komputera — zawiera informacje o statusach ochrony ważnych plików na poszczególnych komputerach wybranego klienta.



Aby zacząć chronić niechronione pliki, zatrzymaj wskaźnik myszy na bloku i kliknij **Chroń wszystkie pliki**. W tym oknie dialogowym znajdziesz informacje o liczbie niechronionych plików i ich lokalizacjach. Aby objąć te pliki ochroną, kliknij **Chroń wszystkie pliki**.

Możesz też pobrać szczegółowy raport w formacie CSV.

Widżety dotyczące oceny luk w zabezpieczeniach

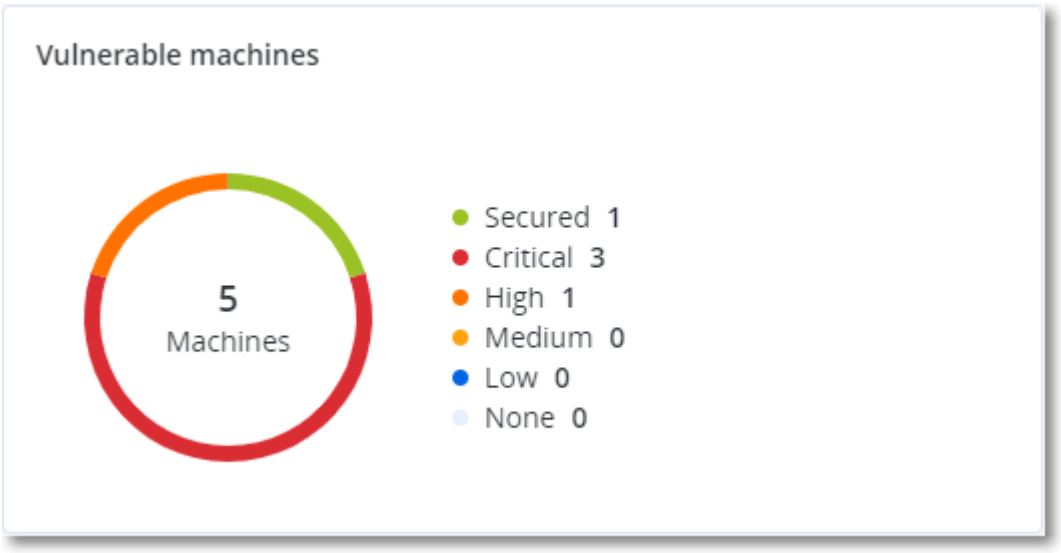
Komputery z lukami w zabezpieczeniach

Ten widżet przedstawia komputery z lukami w zabezpieczeniach uporządkowane według ważności luk.

© Acronis International GmbH, 2003-2024

Znaleziona luka może mieć jeden z następujących poziomów ważności określony zgodnie z systemem Common Vulnerability Scoring System (CVSS) w wersji 3.0:

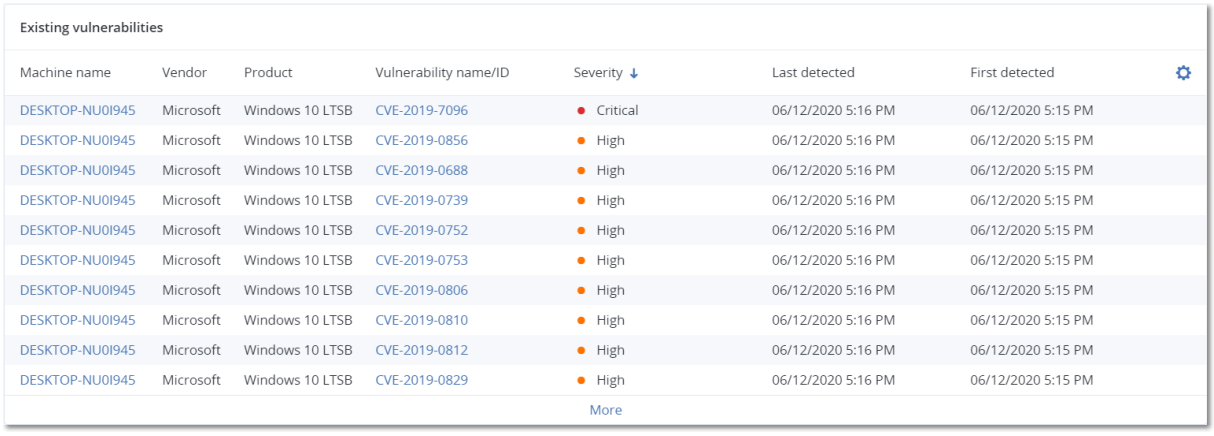
- Bezpieczny: nie znaleziono luk w zabezpieczeniach
- Krytyczny: 9,0–10,0 w skali CVSS
- Wysoki: 7,0–8,9 w skali CVSS
- Średni: 4,0–6,9 w skali CVSS
- Niski: 0,1–3,9 w skali CVSS
- Brak: 0,0 w skali CVSS



Występujące luki w zabezpieczeniach

Ten widżet przedstawia obecnie występujące luki w zabezpieczeniach na komputerach. W widżecie **Istniejące luki w zabezpieczeniach** są dostępne dwie kolumny z sygnaturami czasowymi:

- **Pierwsze wykrycie** — data i godzina pierwszego wykrycia luki na komputerze.
- **Ostatnie wykrycie** — data i godzina ostatniego wykrycia luki na komputerze.


Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

© Acronis International GmbH, 2003-2024

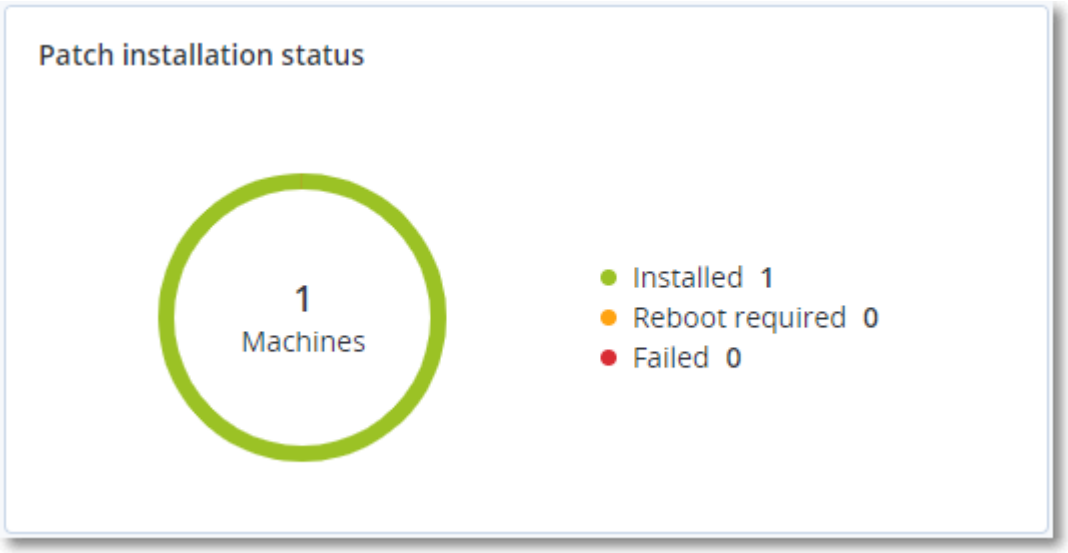
Widżety dotyczące instalacji poprawek

Występują cztery widżety związane z funkcjami zarządzania poprawkami.

Status instalacji poprawek

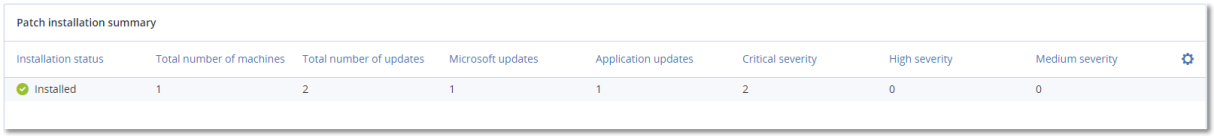
Ten widżet przedstawia liczbę komputerów pogrupowanych według statusów instalacji poprawek.

- **Zainstalowane** — na komputerze zainstalowano wszystkie dostępne poprawki
- **Wymagane ponowne uruchomienie** — po zainstalowaniu poprawki wymagane jest ponowne uruchomienie komputera
- **Niepowodzenie** — instalacja poprawki zakończyła się niepowodzeniem



Podsumowanie instalacji poprawek

Ten widżet przedstawia podsumowanie poprawek na komputerach według statusów ich instalacji.



Historia instalacji poprawek

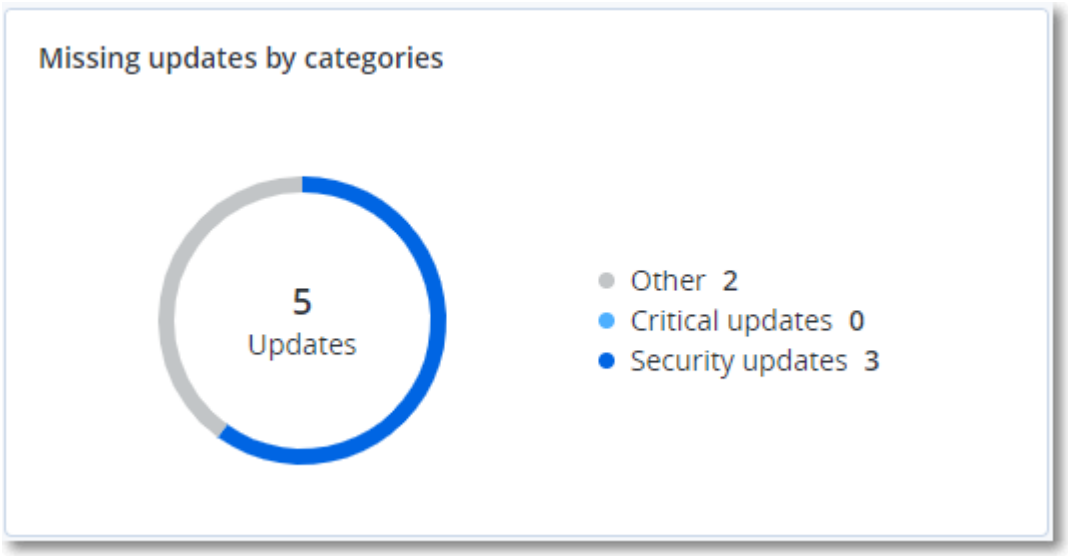
Ten widżet przedstawia szczegółowe informacje o poprawkach na komputerach.

© Acronis International GmbH, 2003-2024

Brakujące aktualizacje według kategorii

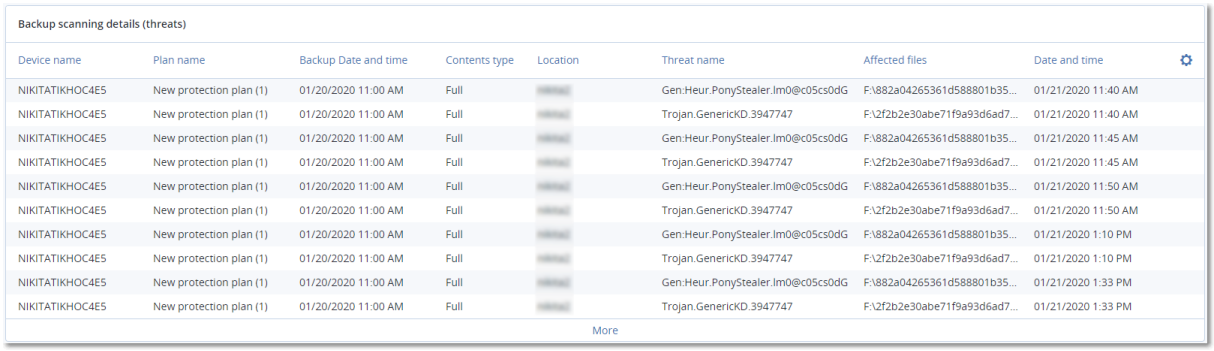
Ten widżet przedstawia liczbę brakujących aktualizacji według kategorii. Pokazywane są następujące kategorie:

- Aktualizacje zabezpieczeń
- Aktualizacje krytyczne
- Inne



Szczegóły skanowania kopii zapasowej

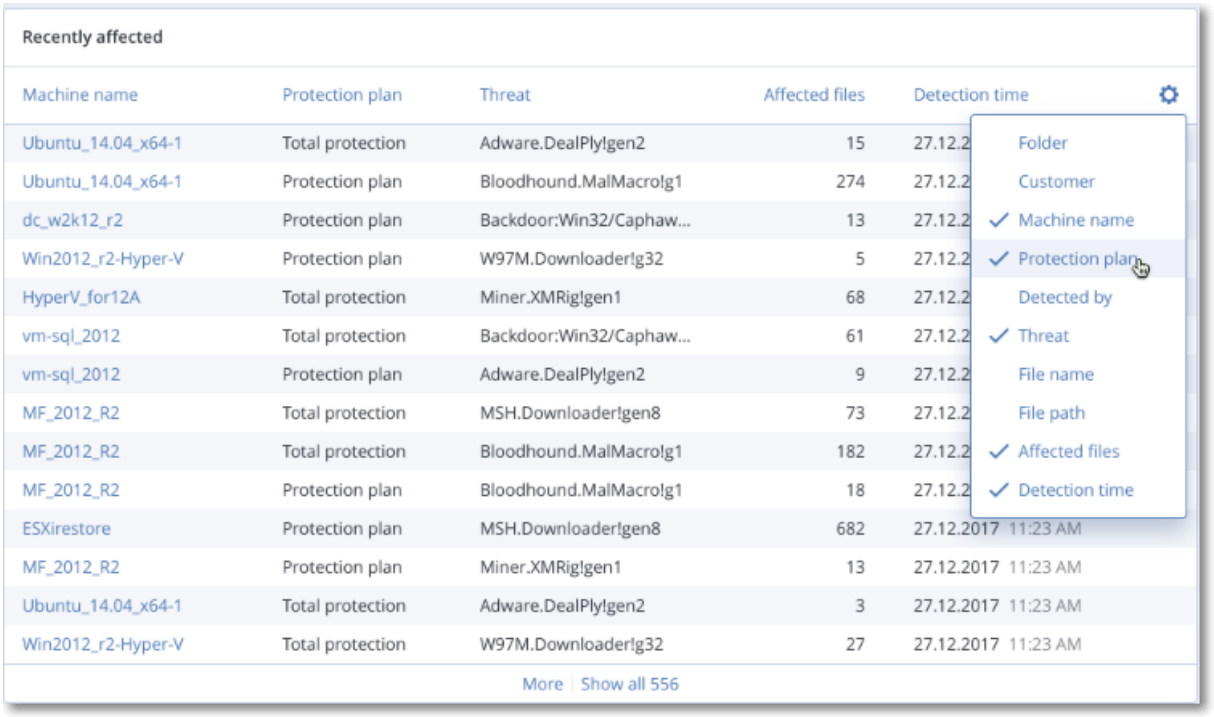
Ten widżet przedstawia szczegółowe informacje o wykrytych zagrożeniach w kopiach zapasowych.



© Acronis International GmbH, 2003-2024

Ostatnio dotknięte problemem

Ten widżet przedstawia szczegółowe informacje o obciążeniach, które ucierpiały wskutek zagrożeń, takich jak wirusy, złośliwe oprogramowanie czy ramsomware. Dostępne są informacje o wykrytych zagrożeniach, czasie ich wykrycia oraz liczbie plików, na które miały one wpływ.



Pobieranie danych dotyczących ostatnio dotkniętych problemem obciążeń

Można pobrać dane dotyczące ostatnio dotkniętych problemem obciążeń, wygenerować plik CSV i wysłać go do wskazanych odbiorców.

Aby pobrać dane dotyczące ostatnio dotkniętych problemem obciążeń

1. W widżecie **Ostatnio dotknięte problemem** kliknij **Pobierz dane**.
2. W polu **Okres** wprowadź liczbę dni, których mają dotyczyć pobierane dane. Można wprowadzić maksymalnie 200 dni.
3. W polu **Odbiorcy** wprowadź adresy e-mail wszystkich osób, które otrzymają wiadomość e-mail z łączem umożliwiającym pobranie pliku CSV.
4. Kliknij **Pobierz**.

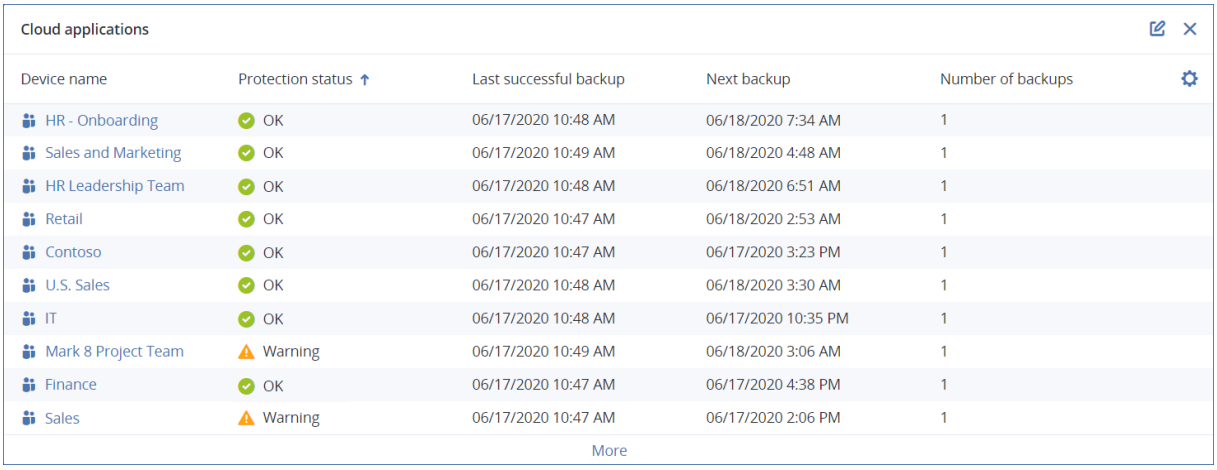
   System zacznie generować plik CSV z danymi dotyczącymi obciążeń, które zostały dotknięte problemem we wskazanym okresie. Gdy plik CSV będzie gotowy, system wyśle wiadomość e-mail do odbiorców. Każdy odbiorca będzie mógł pobrać ten plik CSV.

Aplikacje w chmurze

Ten widżet przedstawia szczegółowe informacje o zasobach obsługiwanych między chmurami:

© Acronis International GmbH, 2003-2024

- Użytkownicy pakietu Microsoft 365 (skrzynka pocztowa, OneDrive)
- Grupy z pakietu Microsoft 365 (skrzynka pocztowa, witryna grupy)
- Foldery publiczne Microsoft 365
- Zbiory witryn Microsoft 365
- Microsoft 365 Teams
- Użytkownicy Google Workspace (Gmail, Dysk Google)
- Dyski współdzielone Google Workspace



Dodatkowe informacje na temat zasobów obsługiwanych między chmurami są też dostępne w następujących widżetach:

- Działania
- Lista działań
- 5 ostatnich alertów
- Historia alertów
- Podsumowanie aktywnych alertów
- Historyczne zestawienie alertów
- Szczegóły aktywnych alertów
- Podsumowanie lokalizacji

Widżet inwentaryzacji oprogramowania

W widżecie tabeli **Inwentaryzacja oprogramowania** są wyświetlane szczegółowe informacje na temat wszystkich programów zainstalowanych na urządzeniach organizacji z systemem Windows lub macOS.

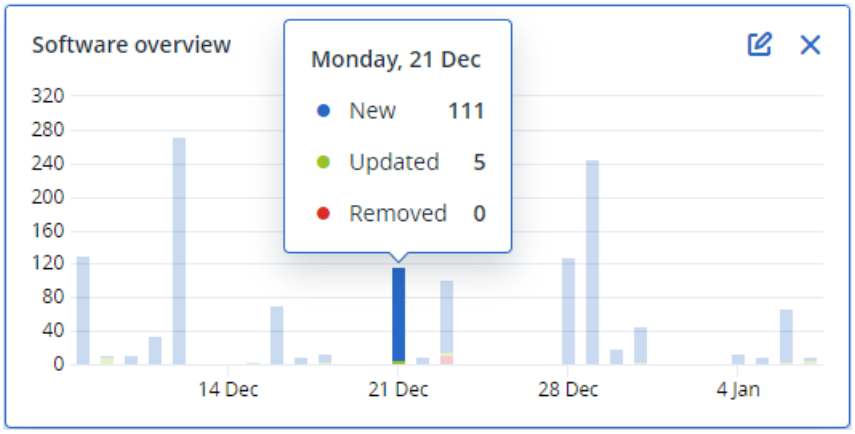
© Acronis International GmbH, 2003-2024

Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
Ivelins-Mac-mini-2.local									
Ivelins-Mac-mini-2.local	-	15.0.26046	-	No change	-	12/12/2020, 3:26 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Pages.app	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Keynote.app	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Numbers.a...	root
Ivelins-Mac-mini-2.local	Canon IJScanner2	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	Canon IJScanner4	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	Canon IJScanner6	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	commandFilter	1.71	EPSON (TXAEAV5RN4)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Printers/EPSON/...	root
Ivelins-Mac-mini-2.local	Cyber Protect Agent Assis...	1	Acronis International Gm...	No change	-	12/12/2020, 10:01 AM	12/14/2020, 10:24 AM	/Applications/Utilities/Cy...	root
Ivelins-Mac-mini-2.local	Cyber Protect Agent Unin...	1	Acronis International Gm...	No change	-	12/12/2020, 3:28 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root

More

W widżecie tabeli **Przegląd oprogramowania** są wyświetlane liczby nowych, zaktualizowanych i usuniętych we wskazanym okresie (7 dni, 30 dni lub bieżący miesiąc) aplikacji na urządzeniach organizacji z systemem Windows lub macOS.



Po wskazaniu myszą określonego słupka wykresu pojawia się etykieta z następującymi informacjami:

Nowe — liczba nowo zainstalowanych aplikacji.

Zaktualizowano — liczba zaktualizowanych aplikacji.

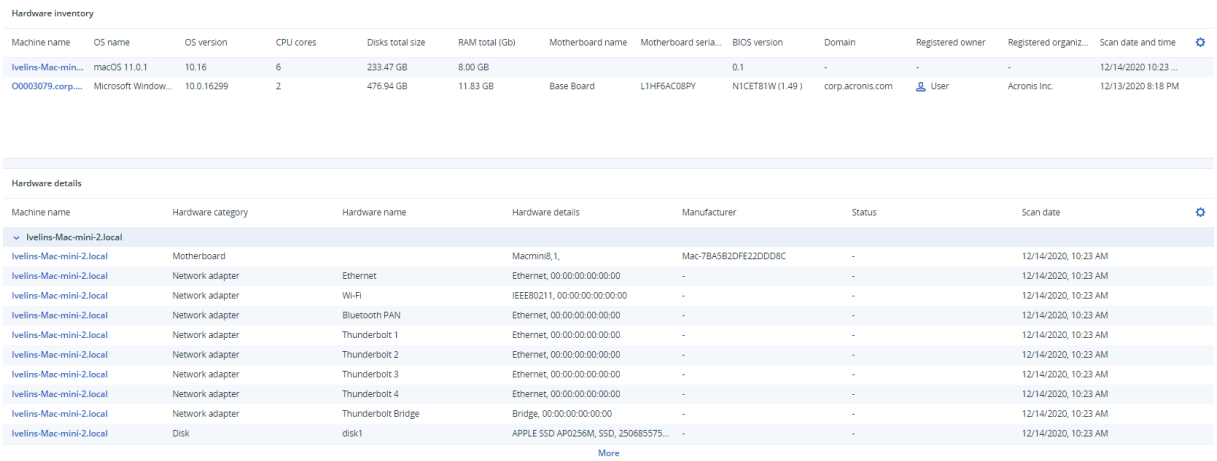
Usunięto — liczba usuniętych aplikacji.

Po kliknięciu części słupka odpowiadającej danemu statusowi nastąpi przekierowanie do strony **Zarządzanie oprogramowaniem** -> **Inwentaryzacja oprogramowania**. Informacje dostępne na tej stronie są filtrowane według odpowiedniej daty i statusu.

Widżety inwentaryzacji sprzętu

W widżetach tabeli **Inwentaryzacja sprzętu** i **Szczegóły sprzętu** są pokazywane informacje na temat wszystkich elementów sprzętowych zainstalowanych w fizycznych i wirtualnych urządzeniach z systemem Windows lub macOS należących do Twojej organizacji.

© Acronis International GmbH, 2003-2024



Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

W widżecie tabeli **Zmiany sprzętowe** są wyświetlane informacje na temat sprzętu w należących do Twojej organizacji fizycznych i wirtualnych urządzeniach z systemem Windows lub macOS, który dodano, usunięto i zmieniono we wskazanym okresie (7 dni, 30 dni lub bieżący miesiąc).

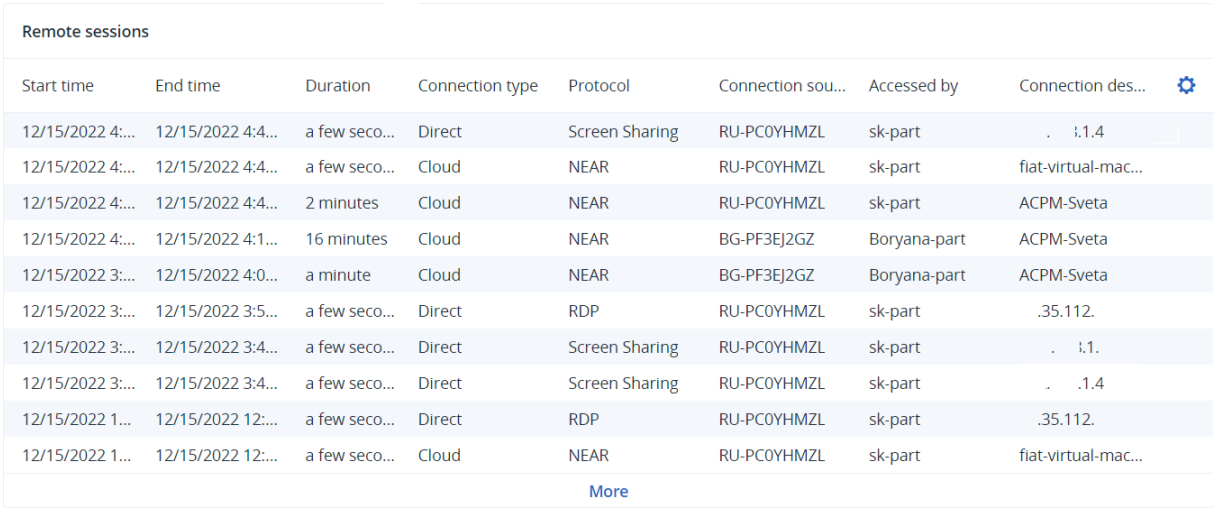
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

Widżet Sesje zdalne

Ten widżet umożliwia wyświetlenie szczegółowych informacji o sesjach pulpitu zdalnego i przesyłania plików.



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

© Acronis International GmbH, 2003-2024

Inteligentna ochrona

Kanał dotyczący zagrożeń

Acronis Cyber Protection Operations Center (CPOC) generuje alerty bezpieczeństwa i wysyła je tylko do tych regionów geograficznych, których te alerty dotyczą. Alerty zawierają informacje o złośliwym oprogramowaniu, lukach w zabezpieczeniach, klęskach żywiołowych, zagrożeniach zdrowia publicznego i innych rodzajach zdarzeń globalnych, które mogą mieć wpływ na ochronę Twoich danych. Kanał dotyczący zagrożeń zawiera informacje o wszelkich potencjalnych zagrożeniach i pozwala im zapobiegać.

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Niektóre problemy sygnalizowane przez alerty ochrony mogą zostać rozwiązane przy użyciu poniższego zestawu konkretnych czynności podejmowanych przez ekspertów ds. ochrony. Inne alerty ochrony stanowią tylko powiadomienia o nadchodzących zagrożeniach — w ich przypadku nie są zalecane żadne działania.

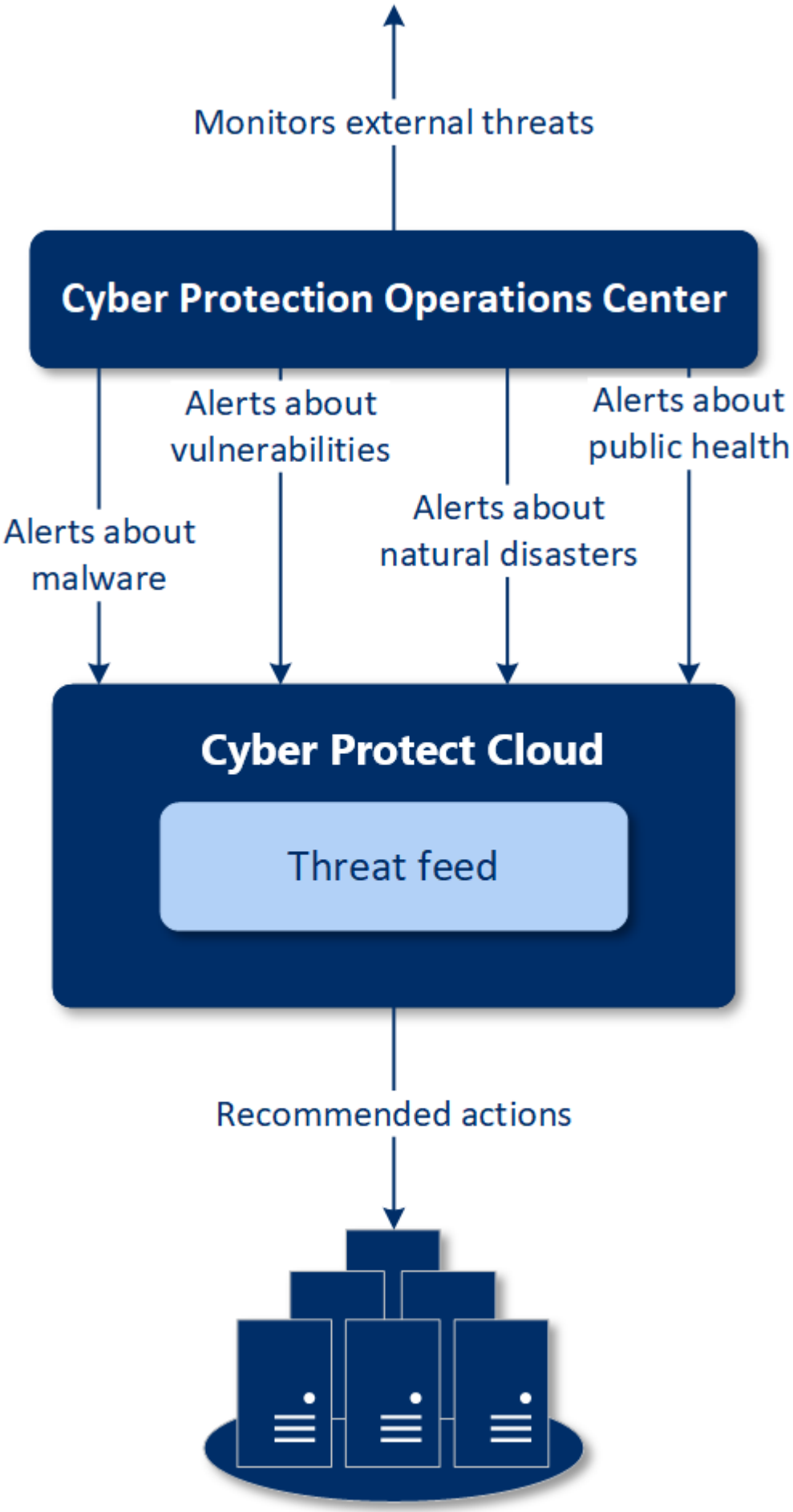
Uwaga
Alerty dotyczące złośliwego oprogramowania są generowane tylko w przypadku komputerów, na których zainstalowano agenta dla usługi Ochrona przed złośliwym oprogramowaniem.

Sposób działania

Acronis Cyber Protection Operations Center monitoruje zewnętrzne zagrożenia i generuje alerty o złośliwym oprogramowaniu, lukach w zabezpieczeniach, zagrożeniach klęskami żywiołowymi i zagrożeniach zdrowia publicznego. Wszystkie te alerty będą widoczne w konsoli Cyber Protect — w sekcji **Kanał dotyczący zagrożeń**. W zależności od rodzaju alertu można podjąć odpowiednie zalecane działania.

Na poniższym schemacie przedstawiono główny przepływ roboczy kanału dotyczącego zagrożeń.

© Acronis International GmbH, 2003-2024



© Acronis International GmbH, 2003-2024

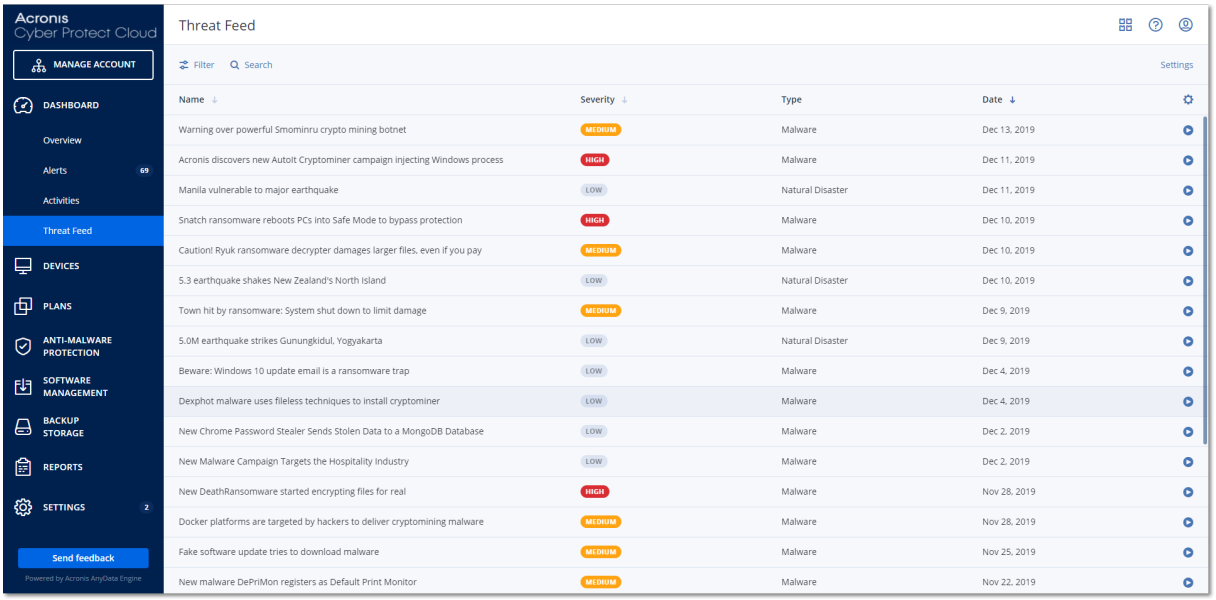
Aby wykonać zalecane działania w przypadku otrzymanych alertów z Acronis Cyber Protection Operations Center:

1. W konsoli Cyber Protect przejdź do sekcji **Monitorowanie** > **Kanał dotyczący zagrożeń** i przejrzyj ewentualne wygenerowane alerty bezpieczeństwa.
2. Wybierz alert z listy i zapoznaj się z jego szczegółami.
3. Kliknij **Rozpocznij**, aby uruchomić kreator.
4. Włącz opcje działań do wykonania oraz komputerów, do których te działania mają zastosowanie. Mogą zostać zaproponowane następujące działania:
   - **Ocena luk w zabezpieczeniach** — przeskanowanie komputerów pod kątem luk w zabezpieczeniach
   - **Zarządzanie poprawkami** — zainstalowanie poprawek na wybranych komputerach
   - **Ochrona antywirusowa** — przeprowadzenie pełnego skanowania wybranych komputerów

     Uwaga
     Ta czynność jest dostępna tylko w przypadku komputerów, na których zainstalowano agenta Ochrony przed złośliwym oprogramowaniem.

   - **Twórz kopie zapasowe chronionych lub niechronionych komputerów** — utworzenie kopii zapasowych chronionych i niechronionych obciążeń.
     Jeśli nie ma jeszcze żadnej kopii zapasowej danego obciążenia (w żadnej z dostępnych lokalizacji, zarówno w chmurze, jak i lokalnie), system utworzy pełną kopię zapasową o nazwie w następującym formacie:
     `%workload_name%-Remediation`
     Domyślnie miejscem docelowym kopii zapasowej jest magazyn usługi Cyber Protect Cloud, ale przed rozpoczęciem operacji można skonfigurować inną lokalizację.
     Jeśli już istnieje niezaszyfrowana kopia zapasowa, system utworzy przyrostową kopię zapasową w już istniejącym archiwum.
5. Kliknij **Rozpocznij**.
6. Na stronie **Działania** sprawdź, czy dane działanie zostało pomyślnie wykonane.

© Acronis International GmbH, 2003-2024



Usuwanie wszystkich alertów

Automatyczne oczyszczanie alertów z kanału dotyczącego zagrożeń odbywa się po następujących okresach:

- Katastrofa naturalna — 1 tydzień
- Luka w zabezpieczeniach — 1 miesiąc
- Złośliwe oprogramowanie — 1 miesiąc
- Zdrowie publiczne — 1 tydzień

Mapa ochrony danych

Funkcja Mapa ochrony danych umożliwia:

- Dostęp do szczegółowych informacji na temat przechowywanych na komputerach danych (klasyfikacja, lokalizacja, status ochrony i dodatkowe informacje).
- Wykrywanie, czy dane są chronione. Dane są uznawane za chronione, jeśli są uwzględniane w tworzonych kopiach zapasowych (plan ochrony z włączonym modułem Kopia zapasowa).
- Wykonywanie działań zapewniających ochronę danych.

Sposób działania

1. Najpierw tworzysz plan ochrony z włączonym modułem Mapa ochrony danych.
2. Następnie, po wykonaniu planu oraz wykryciu i przeanalizowaniu danych uzyskujesz wizualną reprezentację ochrony danych w widżecie Mapa ochrony danych.
3. Możesz też przejść do sekcji **Urządzenia** > **Mapa ochrony danych** i znaleźć tam informacje o niechronionych plikach na poszczególnych urządzeniach.
4. Można podjąć działania w celu ochrony wykrytych niechronionych plików na urządzeniach.

© Acronis International GmbH, 2003-2024

Zarządzanie wykrytymi niechronionymi plikami

Aby chronić ważne pliki, które zostały wykryte jako niechronione:

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Mapa ochrony danych**.
   Na liście urządzeń są dostępne ogólne informacje o liczbie niechronionych plików, rozmiarze takich plików na poszczególnych urządzeniach oraz o ostatniej operacji wykrywania danych.
   Aby chronić pliki na danym komputerze, kliknij ikonę wielokropka, a następnie kliknij **Chroń wszystkie pliki**. Nastąpi przekierowanie do listy planów, gdzie można utworzyć plan ochrony z włączonym modułem Kopia zapasowa.
   Aby usunąć z listy określone urządzenie z niechronionymi plikami, kliknij **Ukryj do następnego wykrywania danych**.
2. Aby wyświetlić bardziej szczegółowe informacje o niechronionych plikach na danym urządzeniu, kliknij jego nazwę.
   Zobaczysz liczbę niechronionych plików z podziałem według rozszerzeń i lokalizacji. Wpisz w polu wyszukiwania rozszerzenia, w których przypadku chcesz poznać informacje o niechronionych plikach.
3. Aby objąć ochroną wszystkie niechronione pliki, kliknij **Chroń wszystkie pliki**. Nastąpi przekierowanie do listy planów, gdzie można utworzyć plan ochrony z włączonym modułem Kopia zapasowa.

Aby uzyskać informacje o niechronionych plikach w formie raportu, kliknij **Pobierz szczegółowy raport w formacie CSV**.

Ustawienia modułu Mapa ochrony danych

Więcej informacji na temat tworzenia planu ochrony z wykorzystaniem modułu Mapa ochrony danych można znaleźć w sekcji „Tworzenie planu ochrony".

W przypadku modułu Mapa ochrony danych można określić następujące ustawienia.

Harmonogram

Możesz zdefiniować różne ustawienia w celu utworzenia harmonogramu, według którego będzie wykonywane zadanie Mapy ochrony danych.

Pole	Opis
Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń	To ustawienie umożliwia określenie czasu uruchomienia zadania. Dostępne są następujące wartości: • **Zaplanuj według czasu** — jest to ustawienie domyślne. Zadanie zostanie uruchomione w określonym czasie. • **Gdy użytkownik zaloguje się w systemie** — domyślnie zalogowanie się dowolnego użytkownika spowoduje wyzwolenie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.

© Acronis International GmbH, 2003-2024

Pole	Opis
	• **Gdy użytkownik wyloguje się z systemu** — domyślnie wylogowanie się dowolnego użytkownika spowoduje wyzwolenie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika. **Uwaga** Zadanie nie zostanie uruchomione przy zamykaniu systemu. Zamknięcie systemu i wylogowanie to różne zdarzenia w konfiguracji harmonogramu. • **Podczas uruchamiania systemu** — zadanie zostanie uruchomione podczas uruchamiania systemu operacyjnego. • **Podczas zamknięcia systemu** — zadanie zostanie uruchomione podczas zamykania systemu operacyjnego.
Typ harmonogramu	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Dostępne są następujące wartości: • **Co miesiąc** — należy wybrać miesiące i tygodnie lub dni miesiąca, w których zadanie będzie uruchamiane. • **Codziennie** — jest to ustawienie domyślne. Wybierz dni tygodnia, w które będzie uruchamiane zadanie. • **Co godzinę** — należy wybrać dni tygodnia, liczbę powtórzeń oraz przedział czasu, w których zadanie będzie uruchamiane.
Czas rozpoczęcia	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu** Wybierz dokładną godzinę, o której zostanie uruchomione zadanie.
Uruchom w podanym okresie	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Ustaw zakres czasu, w którym będzie obowiązywać skonfigurowany harmonogram.
Określ konto użytkownika, którego zalogowanie się w systemie operacyjnym zainicjuje wykonanie zadania	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Gdy użytkownik zaloguje się w systemie**. Dostępne są następujące wartości: • **Dowolny użytkownik** — użyj tej opcji, jeśli chcesz, aby zalogowanie się dowolnego użytkownika powodowało wyzwolenie zadania. • **Następujący użytkownik** — użyj tej opcji, jeśli chcesz, aby tylko

© Acronis International GmbH, 2003-2024

Pole	Opis
	zalogowanie się na określonym koncie użytkownika powodowało wyzwolenie zadania.
Określ konto użytkownika, którego wylogowanie się z systemu operacyjnego zainicjuje wykonanie zadania	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Gdy użytkownik wyloguje się z systemu**. Dostępne są następujące wartości: • **Dowolny użytkownik** — użyj tej opcji, jeśli chcesz, aby wylogowanie się dowolnego użytkownika powodowało wyzwolenie zadania. • **Następujący użytkownik** — użyj tej opcji, jeśli chcesz, aby tylko wylogowanie się z określonego konta użytkownika powodowało wyzwolenie zadania.
Warunki rozpoczęcia	Określ wszystkie warunki, które muszą być jednocześnie spełnione, aby zostało uruchomione zadanie. Warunki rozpoczęcia skanowania pod kątem złośliwego oprogramowania są podobne do warunków uruchomienia modułu **Kopia zapasowa**, które opisano w sekcji „Warunki rozpoczęcia”. Można zdefiniować następujące dodatkowe warunki uruchomienia: • **Rozłóż rozpoczęcie zadania w przedziale czasu** — ta opcja umożliwia zdefiniowanie ram czasowych zadań, aby uniknąć wąskich gardeł na łączach sieciowych. Możesz określić opóźnienie w godzinach lub minutach. Jeśli na przykład domyślną godziną rozpoczęcia jest 10:00, a opóźnienie wynosi 60 minut, to zadanie rozpocznie się między godziną 10:00 a 11:00. • **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu** • **Zablokuj włączanie trybu uśpienia lub hibernacji podczas wykonywania zadania** — ta opcja działa tylko w przypadku komputerów z systemem Windows. • **Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie po** — określ czas, po którym zadanie zostanie uruchomione, bez względu na spełnienie innych warunków rozpoczęcia. **Uwaga** Warunki uruchomienia nie są obsługiwane w systemie Linux.

Reguły dotyczące rozszerzeń i wyjątków

Na karcie **Rozszerzenia** możesz utworzyć listę rozszerzeń plików, które będą uznawane za ważne podczas wykrywania danych i sprawdzane pod kątem statusu ochrony. Podaj rozszerzenia w

© Acronis International GmbH, 2003-2024

następującym formacie:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

Na karcie **Reguły wyjątków** możesz wskazać pliki i foldery, które nie będą sprawdzane pod kątem statusu ochrony podczas wykrywania danych.

- **Ukryte pliki i foldery** — w przypadku wybrania tej opcji ukryte pliki i foldery będą pomijane podczas badania danych.
- **Pliki i foldery systemowe** — w przypadku wybrania tej opcji pliki i foldery systemowe będą pomijane podczas badania danych.

Karta Działania

Karta **Działania** zawiera przegląd działań z ostatnich 90 dni.

Aby przefiltrować działania na pulpicie nawigacyjnym

1. W polu **Nazwa urządzenia** podaj nazwę komputera, na którym jest wykonywane dane działanie.
2. Z listy rozwijanej **Status** wybierz status. Na przykład wykonane pomyślnie, niepowodzenie, w toku itd.
3. Z listy rozwijanej **Zdalnie wykonywane czynności** wybierz czynność. Na przykład stosowanie planu, usuwanie kopii zapasowych, instalowanie aktualizacji oprogramowania.
4. W polu **Ostatnie** ustaw okres działań. Na przykład ostatnie działania, działania z ostatnich 24 godzin lub działania ze wskazanego okresu w ciągu ostatnich 90 dni.
5. Jeśli uzyskasz dostęp do karty **Działania** jako administrator partnera, możesz odfiltrować działania określonego klienta, którym zarządzasz.

Aby dostosować widok na karcie **Działania**, kliknij ikonę koła zębatego i wybierz kolumny do wyświetlenia. Aby móc sprawdzać postęp działań w czasie rzeczywistym, zaznacz pole wyboru **Odświeżaj automatycznie**.

Aby anulować uruchomione działanie, kliknij jego nazwę, a następnie na ekranie **Szczegóły** kliknij **Anuluj**.

Listę działań można przeszukiwać według następujących kryteriów:

- Nazwa urządzenia
  To jest nazwa komputera, na którym jest wykonywane dane działanie.
- Rozpoczęte przez
  To jest konto, na którym rozpoczęto dane działanie.

Działania na pulpicie zdalnym można filtrować według następujących właściwości:

- Utworzenie planu
- Stosowanie planu
- Odwoływanie planu
- Usuwanie planu

© Acronis International GmbH, 2003-2024

- Połączenie zdalne
  - Połączenie pulpitu zdalnego z chmurą przy użyciu protokołu RDP
  - Połączenie pulpitu zdalnego z chmurą przy użyciu protokołu NEAR
  - Połączenie pulpitu zdalnego z chmurą przy użyciu protokołu Udostępnianie ekranu firmy Apple
  - Połączenie pulpitu zdalnego za pośrednictwem klienta internetowego
  - Połączenie pulpitu zdalnego przy użyciu aplikacji Quick Assist
  - Bezpośrednie połączenie pulpitu zdalnego przy użyciu protokołu RDP
  - Bezpośrednie połączenie pulpitu zdalnego przy użyciu protokołu Udostępnianie ekranu firmy Apple
  - Przesyłanie plików
  - Przesyłanie plików przy użyciu aplikacji Quick Assist
- Zdalnie wykonywana czynność
  - Wyłączenie obciążenia
  - Ponowne uruchomienie obciążenia
  - Wylogowanie użytkownika zdalnego na obciążeniu
  - Opróżnienie kosza użytkownika na obciążeniu
  - Przełączenie obciążenia w tryb uśpienia

Cyber Protect Monitor

Cyber Protect Monitor wyświetla informacje o statusie ochrony komputera, na którym jest zainstalowany agent dla systemu Windows lub agent dla komputerów Mac, a także umożliwia użytkownikom konfigurowanie ustawień szyfrowania kopii zapasowych i serwera proxy.

Jeśli na maszynie jest zainstalowany agent dla File Sync & Share, Cyber Protect Monitor zapewnia dostęp do usługi File Sync & Share. Funkcje usługi File Sync & Share są dostępne po obowiązkowym wdrożeniu, podczas którego użytkownicy logują się na własnych kontach File Sync & Share i wybierają osobisty folder synchronizacji. Aby uzyskać więcej informacji na temat agenta dla File Sync & Share, zobacz Podręcznik użytkownika usługi Cyber Files Cloud.

Ważne
Cyber Protect Monitor jest dostępny dla użytkowników, którzy mogą nie mieć uprawnień administracyjnych do rozwiązania Cyber Protection lub usługi File Sync & Share.

Poniższa tabela zawiera zestawienie operacji dostępnych dla użytkowników bez praw administracyjnych.

© Acronis International GmbH, 2003-2024

Zainstalowany agent	Użytkownicy mogą	Użytkownicy nie mogą
Agent dla systemu Windows lub agent dla komputerów Mac	• Stosowanie domyślnego planu ochrony do swoich komputerów • sprawdzać statusy ochrony swoich komputerów • Otrzymywania powiadomień usługi Active Protection • tymczasowo wstrzymywać tworzenie kopii zapasowych swoich komputerów • Konfigurowanie ustawień serwera proxy • Zmienianie ustawień szyfrowania kopii zapasowej **Ostrzeżenie!** Zmiana ustawień szyfrowania w narzędziu Cyber Protect Monitor ma pierwszeństwo przed ustawieniami planu ochrony i wpływa na wszystkie kopie zapasowe komputera. Ta operacja może spowodować niepowodzenie niektórych planów ochrony. Aby uzyskać więcej informacji, zobacz "Szyfrowanie" (s. 474). W przypadku zgubienia lub zapomnienia hasła nie da się odzyskać zaszyfrowanych kopii zapasowych.	• Stosowanie niestandardowych planów ochrony • Zarządzanie planami ochrony, które są już zastosowane
Agent dla systemu Windows i agent dla usługi Sync & Share Agent dla komputerów Mac i agent dla Sync & Share	• synchronizować zawartość między lokalnym folderem synchronizacji a swoim kontem File Sync & Share • Wstrzymaj operacje synchronizacji • Zmień folder synchronizacji • Sprawdź typy plików, których nie można zsynchronizować	• Edytuj typy plików, których nie można zsynchronizować

© Acronis International GmbH, 2003-2024

Konfigurowanie ustawień serwera proxy w narzędziu Cyber Protect Monitor

Istnieje możliwość skonfigurowania ustawień serwera proxy w narzędziu Cyber Protect Monitor. Konfiguracja ta będzie miała wpływ na wszystkie agenty zainstalowane na komputerze.

Aby skonfigurować ustawienia serwera proxy

1. Otwórz Cyber Protect Monitor i kliknij ikonę koła zębatego w prawym górnym rogu.
2. Kliknij **Ustawienia**, a następnie **Serwer proxy**.
3. Włącz przełącznik **Użyj serwera proxy** i wprowadź adres oraz port serwera proxy.
4. [Jeśli dostęp do serwera proxy jest chroniony hasłem] Włącz przełącznik **Wymagane hasło** i wprowadź nazwę użytkownika oraz hasło umożliwiające dostęp do serwera proxy.
5. Kliknij **Zapisz**.

   Ustawienia serwera proxy są zapisywane w pliku `http-proxy.yaml`.

Raporty

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Raport z operacji może zawierać dowolny zestaw widżetów pulpitu nawigacyjnego. Wszystkie widżety przedstawiają skrócone informacje dotyczące całej firmy.

W zależności od typu widżetu raport zawiera dane ze wskazanego zakresu czasu lub z chwili przeglądania bądź generowania raportu. Zobacz "Raportowane dane zależnie od typu widżetu" (s. 310).

Wszystkie widżety historyczne przedstawiają dane z tego samego zakresu czasu. Zakres ten można zmienić w ustawieniach raportów.

Można korzystać z raportów domyślnych lub utworzyć raport niestandardowy.

Możesz raport pobrać lub wysłać pocztą e-mail w formacie XLSX (Excel) bądź PDF.

Zestaw raportów domyślnych zależy od używanej wersji usługi Cyber Protection. Raporty domyślne wymieniono poniżej:

Nazwa raportu	Opis
Wynik #CyberFit według komputerów	Pokazuje wynik #CyberFit oszacowany na podstawie oceny wskaźników zabezpieczeń i konfiguracji poszczególnych komputerów oraz zalecenia dotyczące możliwych udoskonaleń.
Alerty	Zawiera alerty zgłoszone w podanym okresie.

© Acronis International GmbH, 2003-2024

Szczegóły skanowania kopii zapasowej	Zawiera szczegółowe informacje o wykrytych zagrożeniach w kopiach zapasowych.
Codzienne działania	Zawiera zestawienie informacji o działaniach wykonanych w podanym okresie.
Mapa ochrony danych	Zawiera szczegółowe informacje o liczbie, rozmiarze, lokalizacji i statusach ochrony wszystkich ważnych plików na komputerach.
Wykryte zagrożenia	Zawiera szczegółowe informacje o zagrożonych komputerach według liczby zablokowanych zagrożeń oraz o komputerach będących w dobrej kondycji i mających luki w zabezpieczeniach.
Wykryte komputery	Zawiera listę wszystkich komputerów znalezionych w sieci organizacji.
Prognoza kondycji dysków	Zawiera prognozowane terminy awarii dysków HDD/SSD oraz aktualne statusy dysków.
Występujące luki w zabezpieczeniach	Zawiera listę istniejących luk w zabezpieczeniach systemów operacyjnych i aplikacji organizacji. Raport obejmuje również szczegółowe informacje dotyczące zagrożonych komputerów w sieci w przypadku każdego produktu z listy.
Inwentaryzacja oprogramowania	Zawiera informacje na temat programów zainstalowanych na urządzeniach firmy.
Inwentaryzacja sprzętu	Zawiera informacje na temat sprzętu dostępnego w urządzeniach firmy.
Podsumowanie zarządzania poprawkami	Zawiera liczbę brakujących, zainstalowanych i możliwych poprawek. W ramach raportów można wyświetlać bardziej szczegółowe informacje, aby sprawdzać brakujące bądź zainstalowane poprawki oraz informacje na temat wszystkich systemów.
Podsumowanie	Zawiera podsumowanie informacji o chronionych urządzeniach w podanym okresie.
Działania w tygodniu	Zawiera zestawienie informacji o działaniach wykonanych w podanym okresie.
Sesje zdalne	Umożliwia wyświetlenie szczegółowych informacji o sesjach pulpitu zdalnego i przesyłania plików.

Czynności dotyczące raportów

Aby zobaczyć raport, kliknij jego nazwę.

Aby dodać nowy raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Pod listą dostępnych raportów kliknij **Dodaj raport**.
3. [Aby dodać predefiniowany raport] Kliknij nazwę predefiniowanego raportu.

© Acronis International GmbH, 2003-2024

4. [Aby dodać raport niestandardowy] Kliknij **Niestandardowe**, a następnie dodaj widżety do raportu.
5. [Opcjonalnie] Możesz przeciągać widżety, aby zmienić ich rozmieszczenie.

Aby edytować raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport do edycji.
   Możesz wykonać następujące czynności:
   - Zmiana nazwy raportu.
   - Zmiana zakresu czasu wszystkich widżetów w raporcie.
   - Określenie odbiorców raportu i czasu wysłania do nich raportu. Dostępne formaty to PDF i XLSX.

Aby usunąć raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport do usunięcia.
3. Kliknij ikonę wielokropka (...), a następnie kliknij **Usuń**.
4. Potwierdź wybór, klikając **Usuń**.

Aby zaplanować raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport do zaplanowania, a następnie kliknij **Ustawienia**.
3. Włącz przełącznik **Zaplanowane**.
   - Podaj adresy e-mail odbiorców.
   - Wybierz format raportu.

     Uwaga
     Można wyeksportować do 1000 pozycji w formacie PDF i do 10 000 pozycji w formacie XLSX. Sygnatury czasowe w plikach PDF i XLSX są oparte na lokalnym czasie urządzenia.

   - Wybierz język raportu.
   - Skonfiguruj harmonogram.
4. Kliknij **Zapisz**.

Aby pobrać raport

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport, a następnie kliknij **Pobierz**.
3. Wybierz format raportu.

Aby wysłać raport

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport, a następnie kliknij **Wyślij**.
3. Podaj adresy e-mail odbiorców.
4. Wybierz format raportu.
5. Kliknij **Wyślij**.

Aby wyeksportować strukturę raportu

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport.
3. Kliknij ikonę wielokropka (...), a następnie kliknij **Eksportuj**.

W wyniku tych działań struktura raportu zostanie zapisana na komputerze jako plik JSON.

Aby składować dane raportu

Korzystając z tej opcji, można wyeksportować wszystkie dane z niestandardowego okresu — bez ich filtrowania — do pliku CSV i wysłać plik CSV do odbiorcy wiadomości e-mail.

Uwaga
Można wyeksportować do 150 000 pozycji w formacie CSV. Sygnatury czasowe w pliku CSV są oparte na uniwersalnym czasie koordynowanym (UTC).

1. W konsoli Cyber Protect przejdź do sekcji **Raporty**.
2. Na liście raportów wybierz raport, z którego danymi chcesz wykonać zrzut.
3. Kliknij ikonę wielokropka (...), a następnie kliknij **Dane zrzutu**.
4. Podaj adresy e-mail odbiorców.
5. W polu **Zakres czasu** wskaż niestandardowy okres, który chcesz uwzględnić w zrzucie danych.

   Uwaga
   W przypadku dłuższych okresów przygotowywanie plików CSV zajmuje więcej czasu.

6. Kliknij **Wyślij**.

Raportowane dane zależnie od typu widżetu

Ze względu na wyświetlany zakres danych można wyróżnić dwa rodzaje widżetów na pulpicie nawigacyjnym:

- Widżety wyświetlające dane aktualne w chwili przeglądania lub generowania raportu.
- Widżety wyświetlające dane historyczne.

W przypadku skonfigurowania zakresu dat w ustawieniach raportu w celu utworzenia zrzutu danych z pewnego okresu, wybrany zakres czasu będzie miał zastosowanie tylko do widżetów

© Acronis International GmbH, 2003-2024

wyświetlających dane historyczne. W przypadku widżetów wyświetlających dane aktualne w chwili przeglądania lub generowania raportu parametr zakresu czasu nie ma zastosowania.

W poniższej tabeli zamieszczono listę dostępnych widżetów i ich zakresów dat.

Nazwa widżetu	Dane wyświetlane w widżetach i raportach
Wynik #CyberFit według komputerów	Aktualne
5 ostatnich alertów	Aktualne
Szczegóły aktywnych alertów	Aktualne
Podsumowanie aktywnych alertów	Aktualne
Działania	Historyczne
Lista działań	Historyczne
Historia alertów	Historyczne
Statystyki taktyk ataków	Historyczne
Szczegóły skanowania kopii zapasowej (zagrożenia)	Historyczne
Status kopii zapasowej	Historyczne — w kolumnach **Operacje łącznie** i **Liczba pomyślnych operacji** Aktualne — w pozostałych kolumnach
Zablokowane adresy URL	Aktualne
Aplikacje w chmurze	Aktualne
Cyber protection	Aktualne
Mapa ochrony danych	Historyczne
Urządzenia	Aktualne
Wykryte komputery	Aktualne
Przegląd kondycji dysków	Aktualne
Status kondycji dysków według urządzeń fizycznych	Aktualne
Występujące luki w zabezpieczeniach	Historyczne
Zmiany sprzętowe	Historyczne
Szczegóły sprzętu	Aktualne
Inwentaryzacja sprzętu	Aktualne

© Acronis International GmbH, 2003-2024

Historyczne zestawienie alertów	Historyczne
Historia ważności incydentów	Historyczne
Podsumowanie lokalizacji	Aktualne
Brakujące aktualizacje według kategorii	Aktualne
Niechroniony	Aktualne
Historia instalacji poprawek	Historyczne
Status instalacji poprawek	Historyczne
Podsumowanie instalacji poprawek	Historyczne
Status ochrony	Aktualne
Ostatnie objęte wpływem	Historyczne
Sesje zdalne	Historyczne
Wykres spalania dotyczący incydentów bezpieczeństwa	Historyczne
Średni czas rozwiązywania problemu incydentu bezpieczeństwa	Historyczne
Inwentaryzacja oprogramowania	Aktualne
Przegląd oprogramowania	Historyczne
Status zagrożeń	Aktualne
Komputery z lukami w zabezpieczeniach	Aktualne
Status sieciowy obciążeń	Aktualne

© Acronis International GmbH, 2003-2024

Zarządzanie obciążeniami w konsoli Cyber Protect

W tej sekcji opisano, jak można zarządzać obciążeniami w konsoli Cyber Protect.

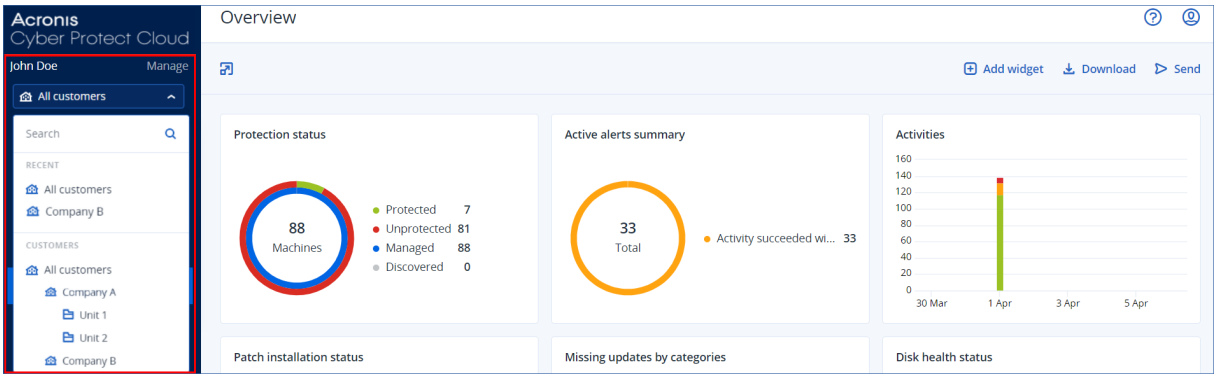
Konsola Cyber Protect

W konsoli Cyber Protect można zarządzać obciążeniami i planami, zmieniać ustawienia ochrony, konfigurować raporty oraz sprawdzać magazyn kopii zapasowych.

Ponadto konsola Cyber Protect zapewnia dostęp do dodatkowych usług lub funkcji, takich jak File Sync & Share, Ochrona przed wirusami i złośliwym oprogramowaniem, Zarządzanie poprawkami, Kontrola urządzeń czy Ocena luk w zabezpieczeniach. Typy i liczba tych usług oraz funkcji zależą od używanej licencji programu Cyber Protection.

Aby sprawdzić pulpit nawigacyjny z najważniejszymi informacjami o ochronie, przejdź do sekcji **Monitorowanie** > **Przegląd**.

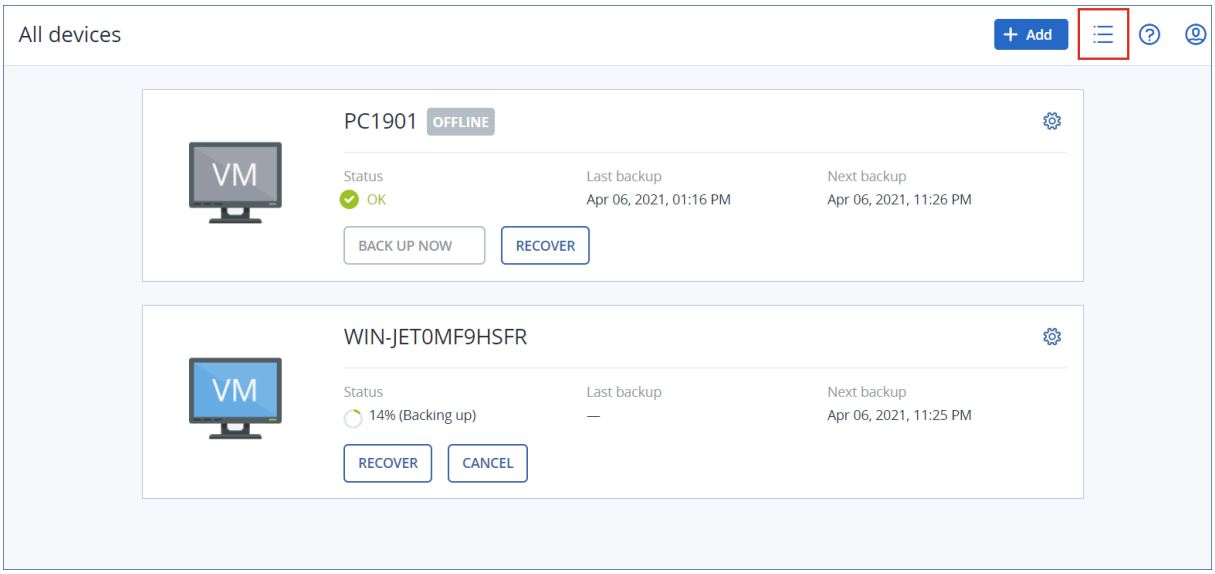
W zależności od uprawnień dostępu możesz zarządzać ochroną jednego lub wielu dzierżawców-klientów bądź jednostek w ramach dzierżawcy. Aby zmienić poziom hierarchii, użyj listy rozwijanej dostępnej w menu nawigacyjnym. Wyświetlane są tylko te poziomy, do których masz dostęp. Aby przejść do portalu zarządzania, kliknij **Zarządzaj**.



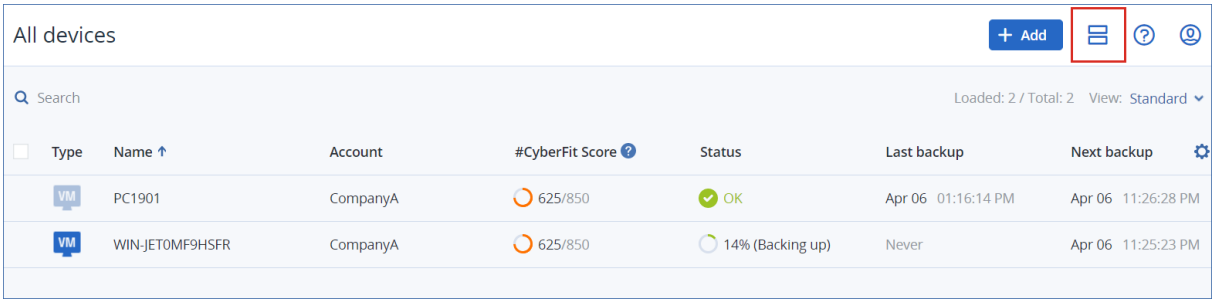
Sekcja **Urządzenia** jest dostępna w prostym widoku tabeli. Aby przełączyć widok, kliknij odpowiednią ikonę w prawym górnym rogu okna.

W widoku prostym jest pokazywanych tylko kilka obciążeń.

© Acronis International GmbH, 2003-2024



W przypadku większej liczby obciążeń automatycznie jest włączany widok tabeli.



Oba widoki zapewniają dostęp do tych samych funkcji i operacji. W niniejszym dokumencie opisano dostęp do operacji z poziomu widoku tabeli.

Kiedy obciążenie przejdzie w tryb online lub offline, trzeba trochę czasu, aby jego status w konsoli Cyber Protect uległ zmianie. Status obciążenia jest sprawdzany co minutę. Jeśli agent zainstalowany na odpowiadającym mu komputerze nie przesyła danych i brak odpowiedzi przez 5 kolejnych operacji sprawdzania, obciążenie będzie wyświetlane jako offline. Obciążenie znów będzie wyświetlane jako online, gdy odpowie na zapytania sprawdzania statusu lub rozpocznie przesyłanie danych.

Co nowego w konsoli Cyber Protect

Jeśli zostaną udostępnione nowe funkcje platformy Cyber Protect Cloud, to po zalogowaniu się do konsoli Cyber Protect zobaczysz wyskakujące okienko z krótkim opisem tych funkcji.

Opis nowych funkcji możesz również zobaczyć, klikając łącze **Co nowego** w lewym dolnym rogu głównego okna konsoli Cyber Protect.

Jeśli nie ma żadnych nowych funkcji, łącze **Co nowego** nie jest wyświetlane.

© Acronis International GmbH, 2003-2024

Korzystanie z konsoli Cyber Protect w przypadku administratora partnera

Jako administrator partnera możesz korzystać z konsoli Cyber Protect na poziomie dzierżawcy-partnera (**Wszyscy klienci**) lub na poziomie dzierżawcy-klienta.

Poziom dzierżawcy-partnera (**Wszyscy klienci**)

Na poziomie dzierżawcy-partnera (**Wszyscy klienci**) możesz wykonywać następujące czynności:

- Zarządzać planami skryptów dla maszyn w ramach wszystkich zarządzanych dzierżawców-klientów.

  Można stosować ten sam plan skryptów do maszyn różnych klientów, a także tworzyć grupy urządzeń z maszynami różnych klientów. Informacje na temat tworzenia statycznej lub dynamicznej grupy urządzeń na poziomie partnera można znaleźć w sekcjach "Tworzenie statycznej grupy urządzeń na poziomie partnera" (s. 318) i "Tworzenie dynamicznej grupy urządzeń na poziomie partnera" (s. 318). Dodatkowe informacje o skryptach i planach skryptów można znaleźć w sekcji "Skrypty cybernetyczne" (s. 398).
- Tworzyć plany monitorowania dotyczące maszyn w ramach wszystkich zarządzanych dzierżawców-klientów.
- Tworzyć plany zarządzania zdalnego dotyczące maszyn w ramach wszystkich zarządzanych dzierżawców-klientów.
- Przeglądaj incydenty wykryte przez usługę Endpoint Detection and Response (EDR) w przypadku wszystkich dzierżawców-klientów i zarządzaj nimi w jednym interfejsie zarządzania incydentami, zamiast uzyskiwać dostęp do ekranu incydentów każdego klienta z osobna.
- Wykonywać automatyczne wykrywanie maszyn w ramach wszystkich zarządzanych dzierżawców-klientów.

Poziom dzierżawcy-klienta

Na tym poziomie masz takie same prawa jak administrator firmy, w którego imieniu działasz.

Wybieranie poziomu dzierżawcy

Możesz wybrać poziom dzierżawcy, na którym chcesz pracować w konsoli Cyber Protect.

Wymagania wstępne

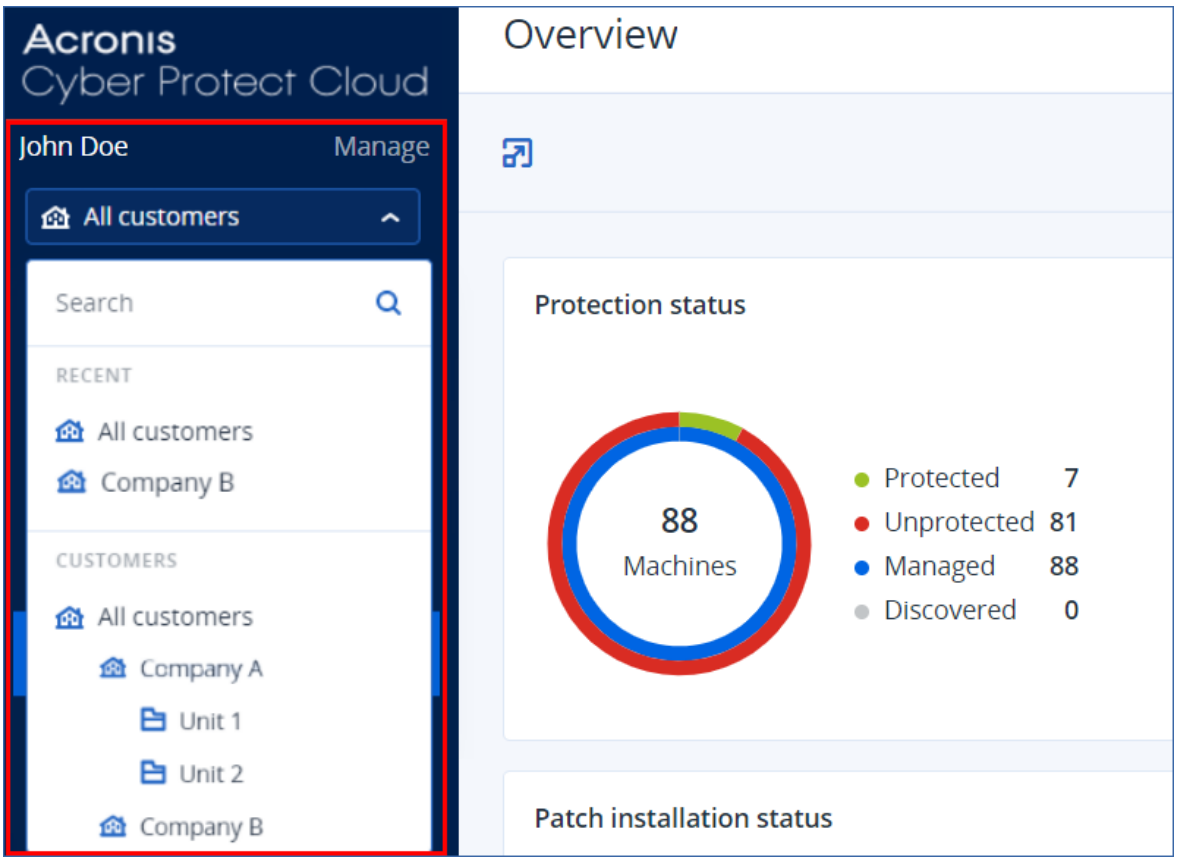
- Masz prawa dostępu do zarówno konsoli Cyber Protect, jak i portalu zarządzania.
- Możesz zarządzać więcej niż jednym dzierżawcą lub jednostką.

Aby wybrać poziom dzierżawcy w konsoli Cyber Protect

1. W menu nawigacyjnym po lewej stronie kliknij strzałkę obok nazwy dzierżawcy-klienta.
2. Wybierz jedną z następujących opcji:

© Acronis International GmbH, 2003-2024

- Jeśli chcesz pracować na poziomie partnera, wybierz **Wszyscy klienci**.
- Jeśli chcesz pracować na poziomie klienta lub jednostki, wybierz nazwę tego klienta lub jednostki.



Poziom dzierżawcy-partnera w konsoli Cyber Protect

Gdy się korzysta z konsoli Cyber Protect na poziomie dzierżawcy-partnera (**Wszyscy klienci**), jest dostępny widok niestandardowy.

Karty **Alerty** i **Działania** udostępniają dodatkowe filtry dotyczące partnerów, a karty **Urządzenia** i **Zarządzanie** — zapewniają dostęp tylko do tych funkcji lub obiektów, które są dostępne dla administratorów partnerów.

Karta Alerty

W tym miejscu można przeglądać alerty pochodzące od wszystkich zarządzanych klientów, wyszukiwać je i filtrować według następujących kryteriów:

- Urządzenie
- Klient
- Plan

W przypadku każdego z tych kryteriów można wybrać wiele pozycji.

© Acronis International GmbH, 2003-2024

Karta Działania

W tym miejscu można przeglądać działania wszystkich zarządzanych dzierżawców lub określonego dzierżawcy-klienta.

Działania można filtrować według klienta, statusu, czasu i typu.

Na tym poziomie są automatycznie wstępnie wybierane następujące typy działań:

- Stosowanie planu
- Tworzenie planu ochrony
- Plan ochrony
- Odwoływanie planu
- Używanie skryptów

Karta Urządzenia

Na karcie **Komputery z agentami** można przeglądać wszystkie obciążenia zarządzanych dzierżawców-klientów, a także wybierać obciążenia jednego lub wielu dzierżawców. Można też tworzyć grupy urządzeń obejmujące obciążenia różnych dzierżawców.

Ważne
Pracując na poziomie partnera (**Wszyscy klienci**), można wykonywać tylko pewną liczbę operacji dotyczących urządzeń. Na przykład nie można wykonać żadnej z następujących operacji:

- Przeglądanie istniejących planów ochrony i zarządzanie nimi na urządzeniach klientów.
- Tworzenie nowych planów ochrony.
- Odzyskiwanie kopii zapasowych.
- Korzystanie z usługi Disaster Recovery.
- Uzyskiwanie dostępu do funkcji narzędzia Cyber Protection Desktop.

Aby wykonać którąkolwiek z tych operacji, trzeba pracować na poziomie klienta.

Karta Zarządzanie oprogramowaniem

Jeśli w przypadku maszyn klienta włączono skanowanie w celu inwentaryzacji ich oprogramowania, masz wgląd w wyniki tego skanowania.

Wyświetlanie maszyn wybranych klientów

Jako administrator partnera możesz wyświetlać maszyny należące do dzierżawców-klientów, którymi zarządzasz.

Aby wyświetlić maszyny wybranego klienta

© Acronis International GmbH, 2003-2024

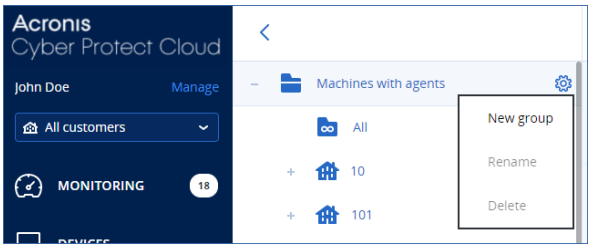
1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. W drzewie kliknij **Komputery z agentami**, aby rozwinąć listę.
3. Kliknij nazwę klienta, którego maszyny chcesz wyświetlić i którego maszynami chcesz zarządzać.

Tworzenie statycznej grupy urządzeń na poziomie partnera

Możesz tworzyć statyczne grupy urządzeń na poziomie partnera (**Wszystkie urządzenia**).

Aby utworzyć statyczną grupę urządzeń na poziomie partnera

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Kliknij ikonę koła zębatego widoczną obok pozycji **Komputery z agentami**, a następnie kliknij **Nowa grupa**.



3. Określ nazwę grupy.
4. [Opcjonalnie] Dodaj opis.
5. Kliknij **OK**.

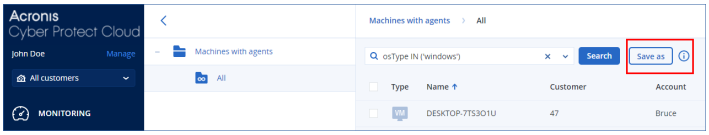
Tworzenie dynamicznej grupy urządzeń na poziomie partnera

Możesz tworzyć dynamiczne grupy urządzeń na poziomie partnera (**Wszystkie urządzenia**).

Aby utworzyć dynamiczną grupę urządzeń na poziomie partnera

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. W drzewie kliknij **Komputery z agentami**, aby rozwinąć listę.
3. Kliknij **Wszystko**.
4. W polu wyszukiwania określ kryteria, według których ma zostać utworzona dynamiczna grupa urządzeń, a następnie kliknij **Szukaj**.

   Dodatkowe informacje na temat dostępnych kryteriów wyszukiwania można znaleźć w sekcjach "Atrybuty wyszukiwania obciążeń innych niż międzychmurowe" (s. 342) i "Atrybuty wyszukiwania obciążeń międzychmurowych" (s. 341).
5. Kliknij **Zapisz jako**, a następnie określ nazwę grupy.



6. [Opcjonalnie] Dodaj opis.
7. Kliknij **OK**.

© Acronis International GmbH, 2003-2024

Wykonywanie automatycznego wykrywania komputerów na poziomie dzierżawcy-partnera

Możesz wykonać automatyczne wykrywanie komputerów na poziomie dzierżawcy-partnera (**Wszyscy klienci**).

Wymagania wstępne

W sieci lokalnej lub domenie Active Directory jest co najmniej jeden komputer z zainstalowanym agentem ochrony.

Ważne
Agentami wykrywania mogą być tylko agenty zainstalowane na komputerach z systemem Windows. Jeśli w środowisku klienta nie ma agentów wykrywania, nie będzie można skorzystać z opcji **Wiele urządzeń** w panelu **Dodaj urządzenia**.

W przypadku dodawania kontrolerów domen wykrywanie automatyczne nie jest obsługiwane z powodu dodatkowych uprawnień wymaganych do uruchomienia usługi agenta.

Zdalna instalacja agentów jest obsługiwana tylko w przypadku komputerów z systemem Windows (system Windows XP nie jest obsługiwany). Aby dokonać instalacji zdalnej na komputerze z systemem Windows Server 2012 R2, musi na nim być zainstalowana aktualizacja systemu Windows KB2999226.

Aby wykonać automatyczne wykrywanie komputerów na poziomie dzierżawcy-partnera

1. W konsoli Cyber Protect wybierz **Wszyscy klienci**.
2. Wybierz kolejno **Urządzenia** > **Wszystkie urządzenia**.
3. Kliknij **Dodaj**.
4. W obszarze **Wiele urządzeń** kliknij **Tylko Windows**. Zostanie uruchomiony Kreator wykrywania automatycznego.
5. Wybierz dzierżawcę-klienta, a następnie wybierz agenta wykrywania, który wykona przeszukiwanie w celu wykrycia komputerów.
6. Wybierz metodę wykrywania:
   - **Szukaj w usłudze Active Directory**. Upewnij się, że komputer z agentem wykrywania należy do domeny Active Directory.
   - **Skanuj sieć lokalną**. Jeśli wybrany agent wykrywania nie znalazł żadnego komputera, wybierz innego agenta wykrywania.
   - **Wpisz ręcznie lub zaimportuj z pliku**. Ręcznie zdefiniuj komputery, które mają zostać dodane, lub zaimportuj je z pliku tekstowego.
7. [Jeśli wybrano metodę wykrywania w domenie Active Directory] Wybierz sposób wyszukiwania komputerów:

© Acronis International GmbH, 2003-2024

- **Na liście jednostek organizacyjnych**. Wybierz grupę komputerów, które mają zostać dodane.
- **Według zapytania w dialekcie LDAP**. Użyj zapytania w dialekcie LDAP, aby wybrać komputery. Opcja **Baza wyszukiwania** umożliwia określenie przeszukiwanych miejsc, a pole **Filtruj** umożliwia podanie kryteriów wyboru komputerów.

8. W zależności od wybranej metody wykrywania wykonaj jedną z następujących czynności:

Metoda wykrywania	Czynność
Szukaj w usłudze Active Directory	Z listy wykrytych komputerów wybierz te, które chcesz dodać.
Skanuj sieć lokalną	Z listy wykrytych komputerów wybierz te, które chcesz dodać.

Wpisz ręcznie lub zaimportuj z pliku	Podaj adresy IP lub nazwy hostów komputerów albo zaimportuj listę komputerów z pliku tekstowego. Plik musi zawierać adresy IP / nazwy hostów zapisane po jednym w każdym wierszu. Oto przykładowy plik:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Po ręcznym dodaniu adresów komputerów lub zaimportowaniu ich z pliku agent próbuje wysłać do dodanych komputerów polecenia ping i ustalić ich dostępność.

9. Wybierz czynności, które muszą zostać podjęte po wykryciu:

Opcja	Opis
Zainstaluj agenty i zarejestruj komputery	Możesz wybrać komponenty, które mają zostać zainstalowane na komputerach, klikając **Wybierz komponenty**. Dodatkowe informacje można znaleźć w sekcji "Wybieranie komponentów do zainstalowania" (s. 189).
Konto logowania dla usługi agenta	To ustawienie jest dostępne na ekranie **Wybierz komponenty**. Ustawienie określa konto, w ramach którego będą uruchamiane usługi. Możesz wybrać jedną z następujących opcji: • **Użyj kont użytkowników usługi** (domyślne w przypadku usługi agenta) Konta użytkowników usługi to konta w systemie Windows używane do uruchamiania usług. Ustawienie to ma tę zaletę, że zasady zabezpieczeń domeny nie wpływają na prawa użytkowników tych kont. Domyślnie agent działa na koncie **System lokalny**. • **Utwórz nowe konto** Nazwą konta dla danego agenta będzie Agent User.

© Acronis International GmbH, 2003-2024

Opcja	Opis
	• **Użyj następującego konta** Jeśli agent zostanie zainstalowany na kontrolerze domeny, system wyświetli monit o określenie istniejących już kont (lub tego samego konta) na potrzeby agenta. Ze względów bezpieczeństwa system nie tworzy automatycznie nowych kont na kontrolerze domeny. W przypadku wybrania opcji **Utwórz nowe konto** lub **Użyj następującego konta** dopilnuj, aby zasady zabezpieczeń domeny nie wpływały na prawa powiązanych kont. Jeśli konto straci prawa użytkownika przypisane podczas instalacji, komponent może działać niepoprawnie lub wcale nie działać.
Zarejestruj komputery z zainstalowanymi agentami	Użyj tej opcji, jeśli agent jest już zainstalowany na komputerach i wystarczy je tylko zarejestrować Cyber Protection. W przypadku nieznalezienia na komputerach żadnego agenta zostaną one dodane jako komputery **Niezarządzane**.
Dodaj jako komputery niezarządzane	W przypadku wybrania tej opcji agent nie zostanie zainstalowany na tych komputerach. Będzie można je przeglądać w konsoli i zainstalować lub zarejestrować agenta później.
W razie potrzeby uruchom ponownie komputer	Ta opcja jest widoczna, gdy została wybrana opcja **Zainstaluj agenty i zarejestruj komputery**. W przypadku wybrania tej opcji komputer zostanie uruchomiony ponownie tyle razy, ile będzie konieczne w celu ukończenia instalacji. Ponowne uruchomienie komputera może być wymagane w jednym z poniższych przypadków: • Ukończono instalację oprogramowania określonego w wymaganiach wstępnych instalacji i trzeba uruchomić ponownie komputer, aby kontynuować instalację. • Ukończono instalację, ale trzeba uruchomić ponownie komputer, ponieważ niektóre pliki zostały zablokowane na czas instalacji. • Ukończono instalację, ale trzeba uruchomić ponownie komputer ze względu na inne wcześniej zainstalowane oprogramowanie.
Nie uruchamiaj ponownie, jeśli jest zalogowany użytkownik	Ta opcja jest widoczna, gdy została wybrana opcja **W razie potrzeby uruchom ponownie komputer**. W przypadku wybrania tej opcji komputer nie zostanie automatycznie uruchomiony ponownie, jeśli użytkownik jest zalogowany w systemie. Jeśli na przykład użytkownik pracuje, gdy instalacja wymaga ponownego uruchomienia, system nie zostanie uruchomiony ponownie. Jeśli wymagane oprogramowanie zostało zainstalowane, ale komputer nie został uruchomiony ponownie ze względu na zalogowaną sesję użytkownika, to w celu ukończenia instalacji należy uruchomić ponownie komputer, a potem jeszcze raz rozpocząć instalację. Jeśli agent został zainstalowany, ale komputer nie został uruchomiony ponownie, należy uruchomić ponownie komputer.

© Acronis International GmbH, 2003-2024

Opcja	Opis
Użytkownik, w ramach którego mają zostać zarejestrowane komputery	[Jeśli organizacja ma jednostki] Wybierz konto użytkownika z jednostki lub jednostek podrzędnych, w ramach którego mają zostać zarejestrowane komputery. [W przypadku wykonywania wykrywania automatycznego na poziomie dzierżawcy-partnera] Na liście dzierżawców-klientów, którymi zarządzasz, rozwiń strukturę drzewa, a następnie wybierz konto użytkownika, w ramach którego chcesz zarejestrować komputery. [W przypadku wykonywania wykrywania automatycznego jako administrator klienta] Jeśli została wybrana opcja **Zainstaluj agenty i zarejestruj komputery** lub **Zarejestruj komputery z zainstalowanymi agentami**, dostępna jest też możliwość zastosowania planu ochrony do komputerów. Jeśli masz kilka planów ochrony, możesz wybrać, którego chcesz użyć.

10. Podaj poświadczenia użytkownika, który ma prawa administratora do wszystkich dodanych komputerów.

    Ważne
    Zdalna instalacja agenta działa bez żadnych przygotowań tylko w przypadku podania poświadczeń dostępu do wbudowanego konta administratora (pierwszego konta utworzonego podczas instalacji systemu operacyjnego). Aby zdefiniować poświadczenia dla niestandardowego administratora, trzeba wykonać dodatkowe przygotowania zgodnie z opisem podanym w sekcji "Wymagania wstępne" (s. 319).

11. System sprawdza możliwość nawiązania połączenia ze wszystkimi komputerami. Jeśli w przypadku jakichś komputerów połączenie się nie powiedzie, można zmienić dotyczące ich poświadczenia.

Po zainicjowaniu operacji wykrywania komputerów odpowiednie zadanie można znaleźć w działaniu **Monitorowanie** > **Działania** > **Wykrywanie komputerów**.

Obsługa wielu dzierżawców

Usługa Cyber Protection obsługuje wielu dzierżawców, co oznacza administrację na następujących poziomach:

- [W przypadku usługodawców] Poziom dzierżawcy-partnera (**Wszyscy klienci**)

  Ten poziom jest dostępny tylko dla administratorów partnerów, którzy zarządzają dzierżawcami-klientami.
- Poziom dzierżawcy-klienta

  Ten poziom jest zarządzany przez administratorów firmy.

  Administratorzy-partnerzy mogą też pracować na tym poziomie w ramach zarządzanych przez siebie dzierżawców-klientów. Na tym poziomie administratorzy partnerów mają takie same prawa jak administratorzy klientów, w których imieniu działają.
- Poziom jednostki

© Acronis International GmbH, 2003-2024

Ten poziom jest zarządzany przez administratorów jednostki oraz administratorów firmy z obszaru nadrzędnego dzierżawcy-klienta.

Administratorzy partnerów, którzy zarządzają nadrzędnym dzierżawcą-klientem, mają również dostęp do poziomu jednostki. Na tym poziomie mają takie same prawa jak administratorzy klientów, w których imieniu działają.

Administratorzy mogą zarządzać obiektami w ramach własnego dzierżawcy oraz jego dzierżawców podrzędnych. Nie widzą obiektów na wyższym poziomie administracji, jeśli taki poziom istnieje, ani nie mogą uzyskiwać do nich dostępu.

Na przykład administratorzy firmy mogą zarządzać planami ochrony zarówno na poziomie dzierżawcy-klienta, jak i na poziomie jednostki. Administratorzy jednostek mogą zarządzać tylko własnymi planami ochrony na poziomie jednostki. Nie mogą oni zarządzać żadnymi planami ochrony na poziomie dzierżawcy-klienta ani planami ochrony utworzonymi przez administratora klienta na poziomie jednostki.

Ponadto administratorzy-partnerzy mogą tworzyć i stosować plany skryptów w ramach zarządzanych przez siebie dzierżawców-klientów. Administratorzy firmy w ramach takich dzierżawców mają dostęp tylko do odczytu do planów skryptów, które są stosowane do ich obciążeń roboczych przez administratora partnerów. Administratorzy klientów mogą jednak tworzyć i stosować własne skrypty lub plany ochrony.

Obciążenia

Obciążenie to chroniony zasób dowolnego typu, na przykład komputer fizyczny, maszyna wirtualna, skrzynka pocztowa lub instancja bazy danych. W konsoli Cyber Protect obciążenie jest wyświetlane jako obiekt, do którego można zastosować plan (plan ochrony, plan tworzenia kopii zapasowych lub plan skryptów).

Niektóre maszyny wymagają zainstalowania agenta ochrony lub wdrożenia urządzenia wirtualnego. Agenty można zainstalować za pomocą graficznego interfejsu użytkownika lub interfejsu wiersza polecenia (instalacja nienadzorowana). Funkcji instalacji nienadzorowanej można użyć w celu zautomatyzowania procedury instalacji. Dodatkowe informacje na temat instalowania agentów ochrony można znaleźć w sekcji "Instalowanie i wdrażanie agentów Cyber Protection" (s. 63).

Urządzenie wirtualne to gotowa maszyna wirtualna, która już zawiera agenta ochrony. Dzięki urządzeniu wirtualnemu można tworzyć kopie zapasowe innych maszyn wirtualnych w tym samym środowisku bez instalowania na nich agenta ochrony (bezagentowe tworzenie kopii zapasowych). Urządzenia wirtualne są dostępne w formatach odpowiednich dla hiperwizora, takich jak .ovf, .ova lub .qcow. Dodatkowe informacje na temat platform wirtualizacji obsługujących bezagentowe tworzenie kopii zapasowych można znaleźć w sekcji "Obsługiwane platformy wirtualizacji" (s. 32).

Ważne

Agenty muszą być w trybie online co najmniej raz na 30 dni. W przeciwnym razie ich plany zostaną odwołane, a obciążenie przestanie być chronione.

Poniższa tabela zawiera zestawienie typów obciążeń i odpowiednich agentów.

© Acronis International GmbH, 2003-2024

Typ obciążenia	Agent	Przykłady (nie jest to lista pełna)
Komputery fizyczne	Agent ochrony jest instalowany na każdym chronionym komputerze.	Stacja robocza Laptop Serwer
Maszyny wirtualne	W zależności od platformy wirtualizacji mogą być dostępne następujące metody tworzenia kopii zapasowych: • Tworzenie kopii zapasowych przy użyciu agenta — agent ochrony jest instalowany na każdym chronionym komputerze. • Bezagentowe tworzenie kopii zapasowych — agent ochrony jest instalowany tylko na hoście hiperwizora lub na specjalnej maszynie wirtualnej albo jest wdrażany jako urządzenie wirtualne. Ten agent tworzy kopie zapasowe wszystkich maszyn wirtualnych znajdujący się w danym środowisku.	Maszyna wirtualna VMware Maszyna wirtualna Hyper-V Środowisko Kernel-based Virtual Machine (KVM) zarządzane przez oVirt
Obciążenia Microsoft 365 Business Obciążenia Google Workspace	Kopie zapasowe tych obciążeń są tworzone przez agenta w chmurze, który nie wymaga instalacji. Aby korzystać z agenta w chmurze, trzeba dodać organizację Microsoft 365 lub Google Workspace do konsoli Cyber Protect. Dodatkowo dostępny jest lokalny agent dla usługi Office 365. Wymaga instalacji i można go używać wyłącznie do tworzenia kopii zapasowych skrzynek pocztowych programu Exchange Online. Dodatkowe informacje na temat różnic między agentem lokalnym a agentem w chmurze można znaleźć w sekcji "Ochrona danych Microsoft 365" (s. 641). .	Skrzynka pocztowa Microsoft 365 Microsoft 365 OneDrive Microsoft Teams Witryna SharePoint Skrzynka pocztowa Google Google Drive
Aplikacje	W przypadku określonych aplikacji kopie zapasowe danych są tworzone przez specjalne agenty, takie jak agent for SQL, agent dla programu Exchange, Agent dla MySQL/MariaDB czy agent dla usługi Active Directory.	Bazy danych programu SQL Server Bazy danych MySQL/MariaDB Bazy danych Oracle Active Directory
Urządzenia mobilne	Na chronionych urządzeniach jest instalowana aplikacja mobilna.	Urządzenia z systemem Android lub iOS

© Acronis International GmbH, 2003-2024

Typ obciążenia	Agent	Przykłady (nie jest to lista pełna)
Witryny internetowe	Kopie zapasowe witryn internetowych są tworzone przez agenta w chmurze, który nie wymaga instalacji.	Witryny internetowe dostępne za pośrednictwem protokołów SFTP lub SSH

Dodatkowe informacje na temat potrzebnego agenta i miejsca jego instalacji można znaleźć w sekcji "Który agent jest potrzebny?" (s. 67)

Dodawanie obciążeń do konsoli Cyber Protect

Aby zacząć chronić swoje obciążenia, należy najpierw dodać je do konsoli Cyber Protect.

Uwaga
Typy obciążeń, które można dodać, zależą od limitów usług dla Twojego konta. Jeśli brakuje określonego typu obciążenia, jest on wyszarzony w panelu **Dodaj urządzenia**.

Administrator partnera może włączyć wymagane limity usług w portalu zarządzania. Szczegółowe informacje można znaleźć w artykule "Informacje dla administratorów partnerów" (s. 329).

Aby dodać obciążenie

1. Zaloguj się do konsoli Cyber Protect.
2. Przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**, a następnie kliknij **Dodaj**.
   Z prawej strony zostanie otwarty panel **Dodaj urządzenia**.
3. Wybierz kanał wersji.
4. Kliknij typ obciążenia, które chcesz dodać, a następnie postępuj zgodnie z instrukcjami dotyczącymi wybranego obciążenia.

Poniższa tabela zawiera zestawienie typów obciążeń i wymaganych czynności.

Obciążenia do dodania	Wymagana czynność	Procedura do wykonania
Wiele komputerów z systemem Windows	Przeprowadź wykrywanie automatyczne w środowisku. Do wykrywania automatycznego potrzebny jest co najmniej jeden komputer z zainstalowanym agentem ochrony w sieci lokalnej lub domenie Active Directory. Agent ten zostanie użyty jako agent wykrywania.	"Wykonywanie automatycznego i ręcznego wykrywania" (s. 183)

© Acronis International GmbH, 2003-2024

Obciążenia do dodania	Wymagana czynność	Procedura do wykonania
Stacje robocze Windows Serwery Windows	Zainstaluj agenta dla systemu Windows.	"Instalowanie agentów ochrony w systemie Windows" (s. 84) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Windows" (s. 92)
Stacje robocze z systemem macOS	Zainstaluj agenta dla systemu macOS.	"Instalowanie agentów ochrony w systemie macOS" (s. 89) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie macOS" (s. 116)
Serwery Linux	Zainstaluj agenta dla systemu Linux.	"Instalowanie agentów ochrony w systemie Linux" (s. 87) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Linux" (s. 110)
Urządzenia mobilne (iOS, Android)	Zainstaluj aplikację mobilną.	"Ochrona urządzeń mobilnych" (s. 633)
Obciążenia międzychmurowe		
Microsoft 365 Business	Dodaj swoją organizację Microsoft 365 do konsoli Cyber Protect i korzystaj z agenta w chmurze w celu ochrony skrzynek pocztowych programu Exchange Online, plików w usłudze OneDrive, instancji Microsoft Teams i witryn SharePoint. Możesz też zainstalować lokalnego agenta dla usługi Office 365. Zapewnia on jedynie tworzenie kopii zapasowych skrzynek pocztowych programu Exchange Online. Dodatkowe informacje na temat różnic między agentem lokalnym a agentem w chmurze można znaleźć w sekcji "Ochrona danych Microsoft 365" (s. 641).	"Ochrona danych Microsoft 365" (s. 641)

© Acronis International GmbH, 2003-2024

Obciążenia do dodania	Wymagana czynność	Procedura do wykonania
Google Workspace	Dodaj swoją organizację Google Workspace do konsoli Cyber Protect i korzystaj z agenta w chmurze w celu ochrony skrzynek pocztowych Gmail i plików na Dysku Google.	"Ochrona danych pakietu Google Workspace" (s. 686)
Maszyny wirtualne		
VMware ESXi	Wdróż w środowisku agenta dla VMware (urządzenie wirtualne).	"Wdrażanie agenta dla VMware (urządzenie wirtualne)" (s. 146)
	Zainstaluj agenta dla VMware (Windows).	"Instalowanie agentów ochrony w systemie Windows" (s. 84) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Windows" (s. 92)
Virtuozzo Hybrid Infrastructure	Wdróż agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne) w danym środowisku.	"Wdrażanie agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne)" (s. 155)
Hyper-V	Zainstaluj agenta dla Hyper-V.	"Instalowanie agentów ochrony w systemie Windows" (s. 84) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Windows" (s. 92)
Virtuozzo	Zainstaluj agenta dla Virtuozzo.	"Instalowanie agentów ochrony w systemie Linux" (s. 87) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Linux" (s. 110)
KVM	Zainstaluj agenta dla systemu Windows.	"Instalowanie agentów ochrony w systemie Windows" (s. 84) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Windows" (s. 92)
	Zainstaluj agenta dla systemu Linux.	"Instalowanie agentów ochrony w

© Acronis International GmbH, 2003-2024

Obciążenia do dodania	Wymagana czynność	Procedura do wykonania
		systemie Linux" (s. 87) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Linux" (s. 110)
Red Hat Virtualization (oVirt)	Wdróż w środowisku agenta dla oVirt (urządzenie wirtualne).	"Wdrażanie agenta dla oVirt (urządzenie wirtualne)" (s. 164)
Citrix XenServer	Zainstaluj agenta dla systemu Windows.	"Instalowanie agentów ochrony w systemie Windows" (s. 84) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Windows" (s. 92)
	Zainstaluj agenta dla systemu Linux.	"Instalowanie agentów ochrony w systemie Linux" (s. 87) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Linux" (s. 110)
Nutanix AHV	Zainstaluj agenta dla systemu Windows.	"Instalowanie agentów ochrony w systemie Windows" (s. 84) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Windows" (s. 92)
	Zainstaluj agenta dla systemu Linux.	"Instalowanie agentów ochrony w systemie Linux" (s. 87) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Linux" (s. 110)
Oracle VM	Zainstaluj agenta dla systemu Windows.	"Instalowanie agentów ochrony w systemie Windows" (s. 84) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie

© Acronis International GmbH, 2003-2024

Obciążenia do dodania	Wymagana czynność	Procedura do wykonania
		Windows" (s. 92)
	Zainstaluj agenta dla systemu Linux.	"Instalowanie agentów ochrony w systemie Linux" (s. 87) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Linux" (s. 110)
Scale Computing HC3	Wdróż w środowisku agenta dla Scale Computing HC3 (urządzenie wirtualne).	"Wdrażanie agenta dla Scale Computing HC3 (urządzenie wirtualne)" (s. 150)
Sieciowa pamięć masowa (NAS)		
Synology	Wdróż w środowisku agenta dla Synology (urządzenie wirtualne).	"Wdrażanie agenta dla Synology" (s. 170)
Aplikacje		
Microsoft SQL Server	Zainstaluj agenta dla SQL.	"Instalowanie agentów ochrony w systemie Windows" (s. 84) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Windows" (s. 92)
Microsoft Exchange Server	Zainstaluj agenta dla programu Exchange.	
Microsoft Active Directory	Zainstaluj agenta dla usługi Active Directory.	
Baza danych Oracle	Zainstaluj agenta dla programu Oracle.	"Ochrona systemu Oracle Database" (s. 712)
Witryna internetowa	Skonfiguruj połączenie z witryną internetową.	"Ochrona witryn internetowych i serwerów hostingu" (s. 720)

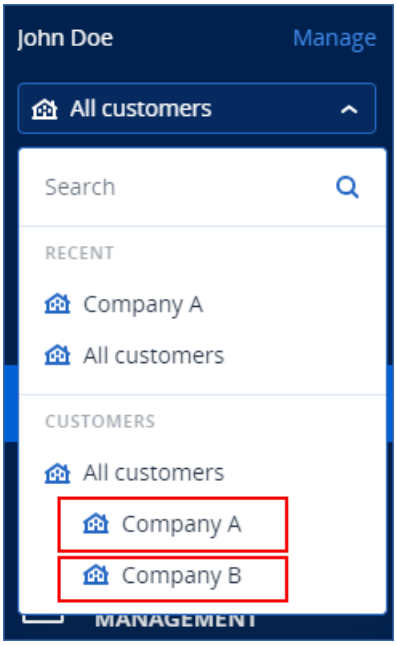
Dodatkowe informacje o dostępnych agentach ochrony i miejscu ich instalacji można znaleźć w sekcji "Który agent jest potrzebny?" (s. 67)

Informacje dla administratorów partnerów

- Jeśli w portalu zarządzania nie włączono wymaganego limitu usługi, to danego typu obciążenia może nie być w panelu **Dodaj urządzenia**. Dodatkowe informacje na temat limitów usług wymaganych w przypadku poszczególnych obciążeń można znaleźć w sekcji Włączanie lub wyłączanie pozycji oferty w Podręczniku administratora partnera.
- Jako administrator partnera nie możesz dodawać obciążeń na poziomie **Wszyscy klienci**. Aby

© Acronis International GmbH, 2003-2024

dodać obciążenie, wybierz określonego dzierżawcę-klienta.



Usuwanie obciążeń z konsoli Cyber Protect

Jeśli jakieś obciążenia już nie wymagają ochrony, można je usunąć z konsoli Cyber Protect. Procedura zależy od typu obciążenia.

Można też odinstalować agenta na chronionym obciążeniu. Po odinstalowaniu agenta chronione obciążenie jest automatycznie usuwane z konsoli Cyber Protect.

Ważne
W przypadku usunięcia obciążenia z konsoli Cyber Protect wszystkie plany zastosowane do tego obciążenia zostaną anulowane. Usunięcie obciążenia nie powoduje usunięcia żadnych planów ani kopii zapasowych i nie powoduje odinstalowania agenta ochrony.

Poniższa tabela zawiera zestawienie typów obciążeń i wymaganych czynności.

Obciążenia do usunięcia	Wymagane czynności	Procedura do wykonania
Komputery fizyczne i maszyny wirtualne		
Komputery fizyczne i maszyny wirtualne z zainstalowanym agentem ochrony	1. Usuń obciążenie z konsoli Cyber Protect. 2. [Opcjonalnie] Odinstaluj agenta ochrony.	"Aby usunąć obciążenie z konsoli Cyber Protect" (s. 332) (Obciążenie z agentem ochrony)
Maszyny	1. W konsoli Cyber	"Aby usunąć obciążenie z konsoli Cyber Protect" (s. 332)

© Acronis International GmbH, 2003-2024

Obciążenia do usunięcia	Wymagane czynności	Procedura do wykonania
wirtualne, których kopie zapasowe są tworzone na poziomie hiperwizora (bezagentowe tworzenie kopii zapasowych)	Protect usuń komputer, na którym jest zainstalowany agent ochrony. Wszystkie maszyny wirtualne, których kopie zapasowe są tworzone przez tego agenta, zostaną automatycznie usunięte z konsoli. 2. [Opcjonalnie] Odinstaluj agenta ochrony.	(Obciążenie bez agenta ochrony)
Obciążenia międzychmurowe		
Obciążenia Microsoft 365 Business Obciążenia Google Workspace	Usuń organizację Microsoft 365 lub Google Workspace z konsoli Cyber Protect. Wszystkie zasoby w ramach tej organizacji zostaną automatycznie usunięte z konsoli.	"Aby usunąć obciążenie z konsoli Cyber Protect" (s. 332) (Obciążenie międzychmurowe)
Urządzenia mobilne		
Urządzenia z systemem Android Urządzenia z systemem iOS	1. Usuń urządzenie mobilne z konsoli Cyber Protect. 2. [Opcjonalnie] Odinstaluj aplikację na urządzeniu mobilnym.	"Aby usunąć obciążenie z konsoli Cyber Protect" (s. 332) (Urządzenie mobilne)
Sieciowa pamięć masowa (NAS)		

© Acronis International GmbH, 2003-2024

Obciążenia do usunięcia	Wymagane czynności	Procedura do wykonania
Synology	1. Usuń obciążenie z konsoli Cyber Protect. 2. [Opcjonalnie] Odinstaluj agenta ochrony.	"Aby usunąć obciążenie z konsoli Cyber Protect" (s. 332) (Obciążenie z agentem ochrony)
Aplikacje		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Baza danych Oracle	1. W konsoli Cyber Protect usuń komputer, na którym jest zainstalowany agent ochrony. Obiekty, których kopie zapasowe są tworzone przez tego agenta, zostaną automatycznie usunięte z konsoli. 2. [Opcjonalnie] Odinstaluj agenta ochrony.	"Aby usunąć obciążenie z konsoli Cyber Protect" (s. 332) (Obciążenie bez agenta ochrony)
Witryny internetowe	Usuń witrynę internetową z konsoli Cyber Protect.	"Aby usunąć obciążenie z konsoli Cyber Protect" (s. 332) (Witryna internetowa)

Aby usunąć obciążenie z konsoli Cyber Protect

Obciążenie z agentem ochrony

Tego typu obciążenie można usunąć bezpośrednio.

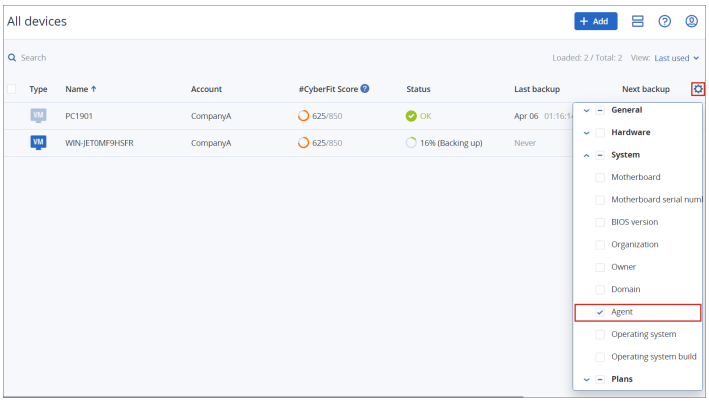
1. W konsoli usługi Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Zaznacz pola wyboru obok obciążeń, które chcesz usunąć.
3. W panelu **Czynności** kliknij **Usuń**.
4. Potwierdź wybór, klikając **Usuń**.
5. [Opcjonalnie] Odinstaluj agenta zgodnie z opisem podanym w sekcji "Odinstalowywanie agentów" (s. 90).

Obciążenie bez agenta ochrony

© Acronis International GmbH, 2003-2024

Aby usunąć obciążenie tego typu, trzeba usunąć komputer, na którym jest zainstalowany agent ochrony.

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. W prawym górnym rogu kliknij ikonę koła zębatego i zaznacz pole wyboru **Agent**.



   Pojawi się kolumna **Agent**.
3. W kolumnie **Agent** sprawdź nazwę komputera, na którym jest zainstalowany dany agent ochrony.
4. W konsoli Cyber Protect zaznacz pole wyboru obok komputera, na którym jest zainstalowany agent ochrony.
5. W panelu **Czynności** kliknij **Usuń**.
6. Potwierdź wybór, klikając **Usuń**.
7. [Opcjonalnie] Odinstaluj agenta zgodnie z opisem podanym w sekcji "Odinstalowywanie agentów" (s. 90).

Obciążenie międzychmurowe

Aby usunąć obciążenia, których kopie zapasowe są tworzone przez agenta w chmurze, usuń swoją organizację Microsoft 365 lub Google Workspace z konsoli Cyber Protect.

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft 365** lub **Urządzenia** > **Google Workspace**.
2. Kliknij nazwę organizacji Microsoft 365 lub Google Workspace.
3. W panelu **Czynności** kliknij **Usuń grupę**.
4. Kliknij **Usuń**, aby potwierdzić czynność.

Urządzenie mobilne

1. W konsoli usługi Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Zaznacz pole wyboru obok obciążenia, które chcesz usunąć.
3. W panelu **Czynności** kliknij **Usuń**.
4. Potwierdź wybór, klikając **Usuń**.
5. [Opcjonalnie] Odinstaluj aplikację na urządzeniu mobilnym.

© Acronis International GmbH, 2003-2024

Witryna internetowa

1. W konsoli usługi Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Zaznacz pole wyboru obok obciążenia, które chcesz usunąć.
3. W panelu **Czynności** kliknij **Usuń**.
4. Potwierdź wybór, klikając **Usuń**.

Grupy urządzeń

Dzięki grupom urządzeń można chronić wiele podobnych obciążeń za pomocą planu grupy. Plan jest stosowany do grupy jako całości i nie można go odwołać w przypadku pojedynczych elementów grupy.

Obciążenie może należeć do więcej niż jednej grupy. Obciążenie należące do grupy urządzeń nadal można chronić przy użyciu planów indywidualnych.

Do grupy urządzeń można dodawać tylko obciążenia tego samego typu. Na przykład w obszarze **Hyper-V** można tworzyć tylko grupy złożone z maszyn wirtualnych Hyper-V. W obszarze **Komputery z agentami** można tworzyć tylko grupy złożone z komputerów z zainstalowanymi agentami.

Grup urządzeń nie można tworzyć w żadnej grupie typu **Wszystkie**, takiej jak grupa główna **Wszystkie urządzenia** czy takie grupy wbudowane jak **Komputery z agentami** > **Wszystkie** lub **Microsoft 365** > Twoja organizacja > **Użytkownicy** > **Wszyscy użytkownicy**.

Grupy wbudowane i grupy niestandardowe

Grupy wbudowane

Po zarejestrowaniu obciążenia w konsoli Cyber Protect będzie ono widoczne w jednej z wbudowanych grup głównych na karcie **Urządzenia**, takich jak **Komputery z agentami**, **Microsoft 365** lub **Hyper-V**.

Wszystkie zarejestrowane obciążenia inne niż międzychmurowe będą widoczne również na liście w grupie głównej **Wszystkie urządzenia**. Osobna wbudowana grupa główna o nazwie takiej samej jak nazwa dzierżawcy zawiera wszystkie obciążenia inne niż międzychmurowe oraz wszystkie jednostki istniejące w ramach tego dzierżawcy.

Nie można usuwać ani edytować grup głównych, a także nie można stosować do nich planów.

Niektóre grupy główne zawierają co najmniej jeden poziom podgrup wbudowanych, na przykład **Komputery z agentami** > **Wszystkie**, **Microsoft 365** > Twoja organizacja > **Zespoły** > **Wszystkie zespoły**, **Google Workspace** > Twoje organizacja > **Dyski współdzielone** > **Wszystkie Dyski udostępnione**.

Podgrup wbudowanych nie można edytować ani usuwać.

© Acronis International GmbH, 2003-2024

Grupy niestandardowe

Ochrona wszystkich obciążeń z grupy wbudowanej może nie być wygodna, ponieważ niektóre z nich mogą wymagać innych ustawień lub harmonogramów ochrony.

W niektórych grupach głównych, na przykład w grupie **Komputery z agentami**, **Microsoft 365** lub **Google Workspace**, można tworzyć podgrupy niestandardowe. Podgrupy te mogą być statyczne lub dynamiczne.

Każdą grupę niestandardową można edytować lub usunąć. Można też zmienić jej nazwę.

Grupy statyczne i grupy dynamiczne

Można tworzyć grupy niestandardowe następujących typów:

- Statyczna
- Dynamiczny

Grupy statyczne

Grupy statyczne zawierają ręcznie dodane obciążenia.

Zawartość grupy statycznej ulegnie zmianie dopiero wtedy, gdy wykonasz operację dodania lub usunięcia obciążenia.

Przykład: Utworzono grupę statyczną dla działu księgowości w firmie, a następnie ręcznie dodano do niej komputery księgowych. Po zastosowaniu planu grupy komputery należące do tej grupy zostały objęte ochroną. Po zatrudnieniu nowego księgowego w tym dziale trzeba będzie ręcznie dodać jego komputer do grupy statycznej.

Grupy dynamiczne

Grupy dynamiczne zawierają obciążenia spełniające określone kryteria. Kryteria te są definiowane najpierw przez utworzenie zapytania, które obejmuje atrybuty (na przykład `osType`), ich wartości (na przykład `Windows`) oraz operatory wyszukiwania (na przykład `W`).

W ten sposób można utworzyć grupę dynamiczną złożoną ze wszystkich komputerów z systemem operacyjnym Windows lub grupę dynamiczną obejmującą wszystkich użytkowników z organizacji Microsoft 365, których adresy e-mail zaczynają się od `jan`.

Każde obciążenie, które ma wymagane atrybuty i wartości, jest automatycznie dodawane do grupy, a każde obciążenie, które utraci wymagany atrybut lub wartość, jest automatycznie usuwane z grupy.

Przykład 1: Nazwy hostów komputerów należących do działu księgowości zawierają słowo księgowość. Wyszukano więc komputery, których nazwy zawierają słowo księgowość, po czym zapisano wyniki wyszukiwania jako grupę dynamiczną. Następnie zastosowano do tej grupy plan ochrony. W przypadku zatrudnienia nowego księgowego jego komputer będzie zawierać słowo

© Acronis International GmbH, 2003-2024

księgowość w nazwie, więc zostanie automatycznie dodany do grupy dynamicznej, gdy tylko zostanie zarejestrowany w konsoli Cyber Protect.

Przykład 2: Dział księgowości stanowi odrębną jednostkę organizacyjną (OU) usługi Active Directory. Wskazano jednostkę organizacyjną „księgowość" jako wymagany atrybut, a następnie zapisano wyniki wyszukiwania jako grupę dynamiczną. Następnie zastosowano do tej grupy plan ochrony. W przypadku zatrudnienia nowego księgowego jego komputer zostanie dodany do grupy dynamicznej, gdy tylko zostanie dodany do jednostki organizacyjnej w usłudze Active Directory i zarejestrowany w konsoli Cyber Protect (nieistotne, co nastąpi najpierw).

Grupy międzychmurowe i inne niż międzychmurowe

Grupy międzychmurowe składają się z obciążeń Microsoft 365 lub Google Workspace, których kopie zapasowe są tworzone za pomocą agenta w chmurze.

Grupy inne niż międzychmurowe zawierają wszystkie inne typy obciążeń.

Plany obsługiwane w przypadku grup urządzeń

W poniższej tabeli zestawiono plany, które można stosować do grup urządzeń.

Grupa	Dostępne plany	Lokalizacja planu
Obciążenia międzychmurowe (obciążenia Microsoft 365 i Google Workspace)	Plan tworzenia kopii zapasowych	**Zarządzanie** > **Kopie zapasowe aplikacji w chmurze**
Obciążenia inne niż międzychmurowe	Plan ochrony	**Zarządzanie** > **Plany ochrony**
	Plan zarządzania zdalnego	**Zarządzanie** > **Plany zarządzania zdalnego**
	Plan skryptów	**Zarządzanie** > **Plany skryptów**

Zasoby w chmurze, takie jak użytkownicy usługi Microsoft 365 lub Google Workspace, OneDrive i Dysk Google, Microsoft Teams lub grupy Azure AD, są synchronizowane z konsolą Cyber Protect zaraz po dodaniu do niej organizacji Microsoft 365 lub Google Workspace. Wszelkie późniejsze zmiany w organizacji są synchronizowane raz dziennie.

Jeśli zajdzie potrzeba niezwłocznej synchronizacji zmiany, w konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft 365** lub **Urządzenia** > **Google Workspace** (stosownie do potrzeb), zaznacz wymaganą organizację, a następnie kliknij **Odśwież**.

Tworzenie grupy statycznej

Możesz utworzyć pustą grupę statyczną i dodać do niej obciążenia.

Możesz też wybrać obciążenia i utworzyć nową grupę statyczną na podstawie dokonanego wyboru.

© Acronis International GmbH, 2003-2024

Grup urządzeń nie można tworzyć w żadnej grupie typu **Wszystkie**, takiej jak grupa główna **Wszystkie urządzenia** czy takie grupy wbudowane jak **Komputery z agentami** > **Wszystkie** lub **Microsoft 365** > Twoja organizacja > **Użytkownicy** > **Wszyscy użytkownicy**.

Aby utworzyć grupę statyczną

W oknie głównym

1. Kliknij **Urządzenia**, a następnie zaznacz grupę główną zawierającą obciążenia, dla których chcesz utworzyć nową grupę statyczną.
2. [Opcjonalnie] Aby utworzyć grupę zagnieżdżoną, przejdź do już istniejącej grupy statycznej.

   Uwaga
   W przypadku obciążeń międzychmurowych nie można tworzyć zagnieżdżonych grup statycznych.

3. Kliknij **+ Nowa grupa statyczna** pod drzewem grup lub kliknij **Nowa grupa statyczna** w panelu **Czynności**.
4. Określ nazwę nowej grupy.
5. [Opcjonalnie] Dodaj komentarz dotyczący grupy.
6. Kliknij **OK**.

W drzewie grup

1. Kliknij **Urządzenia**, a następnie zaznacz grupę główną zawierającą obciążenia, dla których chcesz utworzyć nową grupę statyczną.
2. Kliknij ikonę koła zębatego obok nazwy grupy, w której chcesz utworzyć nową grupę statyczną.

   Uwaga
   W przypadku obciążeń międzychmurowych nie można tworzyć zagnieżdżonych grup statycznych.

3. Kliknij **Nowa grupa statyczna**.
4. Określ nazwę nowej grupy.
5. [Opcjonalnie] Dodaj komentarz dotyczący grupy.
6. Kliknij **OK**.

Na podstawie wyboru

1. Kliknij **Urządzenia**, a następnie zaznacz grupę główną zawierającą obciążenia, dla których chcesz utworzyć nową grupę statyczną.

© Acronis International GmbH, 2003-2024

Uwaga
Grup urządzeń nie można tworzyć w żadnej grupie typu **Wszystkie**, takiej jak grupa główna **Wszystkie urządzenia** czy takie grupy wbudowane jak **Komputery z agentami** > **Wszystkie** lub **Microsoft 365** > Twoja organizacja > **Użytkownicy** > **Wszyscy użytkownicy**.

2. Zaznacz pola wyboru obok obciążeń, dla których chcesz utworzyć nową grupę, a następnie kliknij **Dodaj do grupy**.
3. W drzewie folderów zaznacz poziom nadrzędny nowej grupy, a następnie kliknij **Nowa grupa statyczna**.

Uwaga
W przypadku obciążeń międzychmurowych nie można tworzyć zagnieżdżonych grup statycznych.

4. Określ nazwę nowej grupy.
5. [Opcjonalnie] Dodaj komentarz dotyczący grupy.
6. Kliknij **OK**.
   Nowa grupa pojawi się w drzewie folderów.
7. Kliknij **Gotowe**.

Dodawanie obciążeń do grupy statycznej

Można najpierw wybrać grupę docelową, a następnie dodać do niej obciążenia.

Ewentualnie można najpierw wybrać obciążenia, a następnie dodać je do grupy.

Aby dodać obciążenia do grupy statycznej

Najpierw wybranie grupy docelowej

1. Kliknij **Urządzenia**, a następnie przejdź do odpowiedniej grupy docelowej.
2. Zaznacz grupę docelową, a następnie kliknij **Dodaj urządzenia**.
3. W drzewie folderów wybierz grupę zawierającą wymagane obciążenia.
4. Zaznacz pola wyboru odpowiadające obciążeniom, które mają zostać dodane, a następnie kliknij **Dodaj**.

Najpierw wybranie obciążeń

1. Kliknij **Urządzenia**, a następnie wybierz grupę główną zawierającą wymagane obciążenia.
2. Zaznacz pola wyboru odpowiadające obciążeniom, które mają zostać dodane, a następnie kliknij **Dodaj do grupy**.
3. W drzewie folderów zaznacz grupę docelową, a następnie kliknij **Gotowe**.

© Acronis International GmbH, 2003-2024

Tworzenie grupy dynamicznej

Grupę dynamiczną tworzy się przez wyszukanie obciążeń o określonych atrybutach, których wartości są definiowane w zapytaniu wyszukiwania. Następnie zapisuje się wyniki wyszukiwania jako grupę dynamiczną.

Podczas wyszukiwania i tworzenia grup dynamicznych stosuje się inne atrybuty w przypadku obciążeń międzychmurowych, a inne w przypadku pozostałych obciążeń. Dodatkowe informacje na temat obsługiwanych atrybutów można znaleźć w sekcjach "Atrybuty wyszukiwania obciążeń innych niż międzychmurowe" (s. 342) i "Atrybuty wyszukiwania obciążeń międzychmurowych" (s. 341).

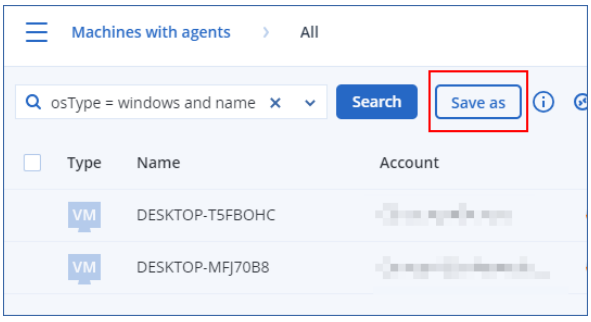
Grupy dynamiczne są tworzone w odpowiadających im grupach głównych. Zagnieżdżone grupy dynamiczne nie są obsługiwane.

Grup urządzeń nie można tworzyć w żadnej grupie typu **Wszystkie**, takiej jak grupa główna **Wszystkie urządzenia** czy takie grupy wbudowane jak **Komputery z agentami** > **Wszystkie** lub **Microsoft 365** > Twoja organizacja > **Użytkownicy** > **Wszyscy użytkownicy**.

Aby utworzyć grupę dynamiczną

Obciążenia inne niż międzychmurowe

1. Kliknij **Urządzenia**, a następnie zaznacz grupę zawierającą obciążenia, dla których chcesz utworzyć nową grupę dynamiczną.
2. Wyszukaj obciążenia przy użyciu obsługiwanych atrybutów i operatorów wyszukiwania.
   W jednym zapytaniu możesz użyć wielu atrybutów i operatorów. Aby uzyskać więcej informacji na temat obsługiwanych atrybutów, zobacz sekcję "Atrybuty wyszukiwania obciążeń innych niż międzychmurowe" (s. 342).
3. Kliknij **Zapisz jako** obok pola wyszukiwania.



Uwaga
Przycisk **Zapisz jako** nie jest dostępny, jeśli nie możesz utworzyć grupy dynamicznej na określonym poziomie. Na przykład w grupie głównej **Urządzenia** > **Wszystkie urządzenia**. Wybierz inny poziom (na przykład **Urządzenia** > **Komputery z agentami** > **Wszystko**), a następnie powtórz powyższe kroki. Dzięki temu wyszukiwaniu możesz utworzyć grupę dynamiczną w ramach grupy **Komputery z agentami**, ale nie w ramach grupy **Komputery z agentami** > **Wszystko**.

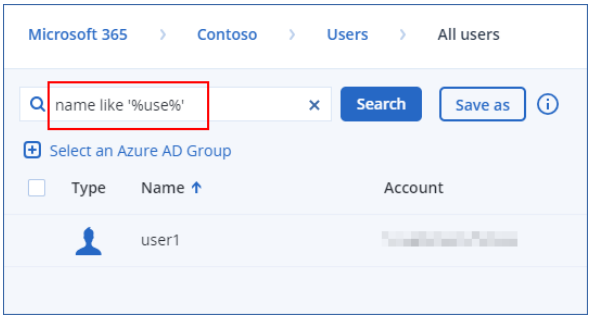
© Acronis International GmbH, 2003-2024

4. Określ nazwę nowej grupy.
5. [Opcjonalnie] W polu **Komentarz** dodaj opis nowej grupy.
6. Kliknij **OK**.

Obciążenia międzychmurowe

1. Kliknij **Urządzenia**, a następnie wybierz **Microsoft 365** lub **Google Workspace**.
2. Wybierz grupę zawierającą maszyny, dla których chcesz utworzyć nową grupę dynamiczną. Na przykład **Użytkownicy** > **Wszyscy użytkownicy**.
3. Wyszukaj obciążenia przy użyciu obsługiwanych atrybutów i operatorów wyszukiwania lub przez wybranie użytkowników usługi Microsoft 365 z określonej grupy usługi Active Directory.

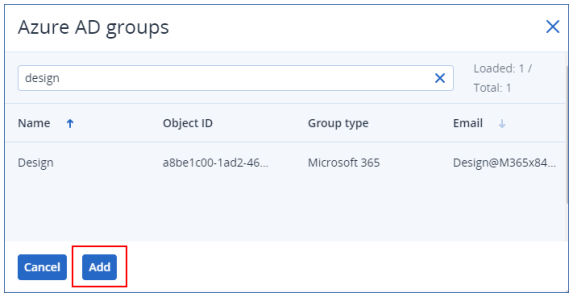
   W jednym zapytaniu możesz użyć wielu atrybutów i operatorów. Aby uzyskać więcej informacji na temat obsługiwanych atrybutów, zobacz sekcję "Atrybuty wyszukiwania obciążeń międzychmurowych" (s. 341).



4. [Tylko w przypadku sekcji **Microsoft 365** > **Użytkownicy**] Aby wybrać użytkowników z określonej grupy usługi Active Directory, wykonaj następujące czynności:
   a. Przejdź do sekcji **Użytkownicy** > **Wszyscy użytkownicy**.
   b. Kliknij **Wybierz grupę usługi Azure AD**.

      Zostanie otwarta lista grup usługi Active Directory istniejących w Twojej organizacji.

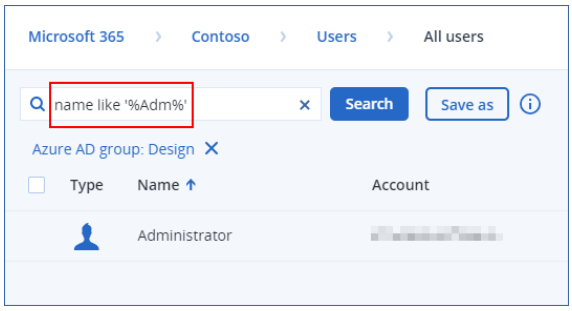
      Na tej liście można wyszukać konkretną grupę lub posortować grupy według nazw bądź adresów e-mail.
   c. Wybierz grupę usługi Active Directory zgodnie ze swoimi preferencjami, a następnie kliknij **Dodaj**.



   d. [Opcjonalnie] Aby uwzględnić lub wykluczyć określonych użytkowników z wybranej grupy usługi Active Directory, utwórz zapytanie wyszukiwania przy użyciu obsługiwanych atrybutów i operatorów wyszukiwania.

© Acronis International GmbH, 2003-2024

W jednym zapytaniu możesz użyć wielu atrybutów i operatorów. Aby uzyskać więcej informacji na temat obsługiwanych atrybutów, zobacz sekcję "Atrybuty wyszukiwania obciążeń międzychmurowych" (s. 341).



5. Kliknij **Zapisz jako** obok pola wyszukiwania.

Uwaga
Przycisk **Zapisz jako** nie jest dostępny, jeśli nie możesz utworzyć grupy dynamicznej na określonym poziomie. Na przykład w grupie **Microsoft 365** > Twoja organizacja > **Użytkownicy**. Wybierz inny poziom (na przykład **Microsoft 365** > Twoja organizacja > **Użytkownicy** > **Wszystko**), a następnie powtórz powyższe kroki. Dzięki temu wyszukiwaniu możesz utworzyć grupę dynamiczną w ramach grupy **Microsoft 365** > Twoja organizacja > **Użytkownicy**, ale nie w grupie **Użytkownicy** > **Wszystko**.

6. Określ nazwę nowej grupy.
7. [Opcjonalnie] W polu **Komentarz** dodaj opis nowej grupy.
8. Kliknij **OK**.

Atrybuty wyszukiwania obciążeń międzychmurowych

W poniższej tabeli zestawiono atrybuty, których można używać w zapytaniach wyszukiwania dotyczących obciążeń Microsoft 365 i Google Workspace.

Aby sprawdzić, jakich atrybutów można używać w zapytaniach wyszukiwania dotyczących innych typów obciążeń, zapoznaj się z sekcją "Atrybuty wyszukiwania obciążeń innych niż międzychmurowe" (s. 342).

Atrybut	Znaczenie	Miejsce zastosowania	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
`name`	Nazwa wyświetlana obciążenia Microsoft 365 lub Google Workspace	Wszystkie zasoby międzychmurowe	`name = 'My Name'` `name LIKE '*nam*'`	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Miejsce zastosowania	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup

`email`	Adres e-mail użytkownika lub grupy w usłudze Microsoft 365 albo użytkownika usługi Google Workspace	Microsoft 365 > Grupy
		Microsoft 365 > Użytkownicy
		Google Workspace > Użytkownicy
			`email = 'my_group_email@mycompany.com'`
			`email LIKE '*@company*'`
			`email NOT LIKE '*enterprise.com'`
				Tak

`siteName`	Nazwa witryny powiązanej z grupą Microsoft 365	Microsoft 365 > Grupy	`siteName = 'my_site'` `siteName LIKE '*company.com*support*'`	Tak
`url`	Adres internetowy witryny grupy Microsoft 365 lub witryny SharePoint	Microsoft 365 > Grupy Microsoft 365 > Zbiory witryn	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	Tak

Atrybuty wyszukiwania obciążeń innych niż międzychmurowe

W poniższej tabeli zestawiono atrybuty, których można używać w zapytaniach wyszukiwania dotyczących obciążeń innych niż międzychmurowe.

Aby sprawdzić, jakich atrybutów można używać w zapytaniach wyszukiwania dotyczących obciążeń międzychmurowych, zapoznaj się z sekcją "Atrybuty wyszukiwania obciążeń międzychmurowych" (s. 341).

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
Ogólne			
`name`	Nazwa obciążenia, na przykład: • Nazwa hosta dla komputerów fizycznych • Nazwa dla maszyn wirtualnych • Nazwa bazy danych • Adres e-mail dla	`name = 'en-00'`	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	skrzynek pocztowych		
`id`	Identyfikator urządzenia. Aby wyświetlić identyfikator urządzenia, w obszarze **Urządzenia** wybierz urządzenie, kliknij **Szczegóły** > **Wszystkie właściwości**. Identyfikator jest pokazywany w polu `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tak
`resourceType`	Typ obciążenia. Możliwe wartości: • `'machine'` • `'exchange'` • `'mssql_server'` • `'mssql_instance'` • `'mssql_database'` • `'mssql_database_folder'` • `'msexchange_database'` • `'msexchange_storage_group'` • `'msexchange_mailbox.msexchange'` • `'msexchange_mailbox.office365'` • `'mssql_aag_group'` • `'mssql_aag_database'` • `'virtual_machine.vmww'` • `'virtual_machine.vmwesx'` • `'virtual_host.vmwesx'` • `'virtual_cluster.vmwesx'` • `'virtual_appliance.vmwesx'` • `'virtual_application.vmwesx'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	• 'virtual_resource_pool.vmwesx' • 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_host.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • 'bootable_media'		
chassis	Typ obudowy. Możliwe wartości:	chassis = 'laptop' chassis IN ('laptop', 'desktop')	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	• `laptop` • `desktop` • `server` • `other` • `unknown`		
`ip`	Adres IP (tylko w przypadku komputerów fizycznych).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Tak
`comment`	Komentarz dotyczący urządzenia. Może on zostać określony automatycznie lub ręcznie. Wartość domyślna: • W przypadku komputerów fizycznych z systemem Windows jest to opis komputera automatycznie skopiowany jako komentarz. Ta wartość jest synchronizowana co 15 minut. • W przypadku innych urządzeń pozostaje pusty. **Uwaga** Jeśli w polu komentarza został ręcznie dodany tekst, synchronizacja automatyczna jest wyłączona. Aby ponownie włączyć synchronizację, wyczyść ten tekst. Aby odświeżyć automatycznie synchronizowane komentarze dotyczące swoich obciążeń, uruchom	`comment = 'important machine'` `comment = ''` (wszystkie komputery bez komentarza)	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup

	ponownie usługę komputera zarządzanego w sekcji **Usługi systemu Windows** lub uruchom w wierszu polecenia następujące polecenia:
	`net stop mms`
	`net start mms`
	Aby wyświetlić komentarz dotyczący urządzenia, wybierz je w obszarze **Urządzenia**, kliknij **Szczegóły**, a następnie znajdź sekcję **Komentarz**.
	Aby ręcznie dodać lub zmienić komentarz, kliknij **Dodaj** lub **Edytuj**.
	W przypadku urządzeń, na których jest zainstalowany agent ochrony, istnieją dwa osobne pola komentarzy:
	• Komentarz dotyczący agenta
	◦ W przypadku komputerów fizycznych z systemem Windows jest to opis komputera automatycznie skopiowany jako komentarz. Ta wartość jest synchronizowana co 15 minut.
	◦ W przypadku innych urządzeń pozostaje		

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	pusty. **Uwaga** Jeśli w polu komentarza został ręcznie dodany tekst, synchronizacja automatyczna jest wyłączona. Aby ponownie włączyć synchronizację, wyczyść ten tekst. • Komentarz dotyczący urządzenia ◦ Jeśli komentarz dotyczący agenta zostanie dodany automatycznie, zostanie on skopiowany jako komentarz dotyczący urządzenia. Ręcznie dodane komentarze dotyczące agenta nie są kopiowane jako komentarze dotyczące urządzenia. ◦ Komentarze dotyczące urządzenia nie są kopiowane jako komentarze dotyczące agenta. W przypadku urządzenia może zostać dodany jeden z tych komentarzy lub oba te komentarze. Pola te mogą też pozostać puste. W przypadku dodania obu tych komentarzy komentarz dotyczący urządzenia ma		

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	pierwszeństwo. Aby wyświetlić komentarz dotyczący agenta, w obszarze **Ustawienia** > **Agenci** wybierz urządzenie z agentem, kliknij **Szczegóły**, a następnie znajdź sekcję **Komentarz**. Aby wyświetlić komentarz dotyczący urządzenia, wybierz je w obszarze **Urządzenia**, kliknij **Szczegóły**, a następnie znajdź sekcję **Komentarz**. Aby ręcznie dodać lub zmienić komentarz, kliknij **Dodaj** lub **Edytuj**.		
`isOnline`	Dostępność obciążenia. Możliwe wartości: • `true` • `false`	`isOnline = true`	Nie
`hasAsz`	Dostępność partycji Secure Zone. Możliwe wartości: • `true` • `false`	`hasAsz = true`	Tak

`tzOffset`	Przesunięcie strefy czasowej względem uniwersalnego czasu koordynowanego (UTC) w minutach.	`tzOffset = 120`
		`tzOffset > 120`
		`tzOffset < 120`
			Tak

Procesor, pamięć, dyski			
`cpuArch`	Architektura CPU. Możliwe wartości:	`cpuArch = 'x64'`	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	• `'x64'` • `'x86'`		
`cpuName`	Nazwa procesora.	`cpuName LIKE '%XEON%'`	Tak
`memorySize`	Rozmiar pamięci RAM w megabajtach.	`memorySize < 1024`	Tak
`diskSize`	Pojemność dysku twardego w giga- lub megabajtach (tylko w przypadku komputerów fizycznych).	`diskSize < 300GB` `diskSize >= 3000000MB`	Nie
System operacyjny			
`osName`	Nazwa systemu operacyjnego.	`osName LIKE '%Windows XP%'`	Tak
`osType`	Typ systemu operacyjnego. Możliwe wartości: • `'windows'` • `'linux'` • `'macosx'`	`osType = 'windows'` `osType IN ('linux', 'macosx')`	Tak
`osArch`	Architektura systemu operacyjnego. Możliwe wartości: • `'x64'` • `'x86'`	`cpuArch = 'x86'`	Tak
`osProductType`	Typ produktu systemu operacyjnego. Możliwe wartości: • `'dc'` Oznacza kontroler domeny.	`osProductType = 'server'`	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	Uwaga Gdy rola kontrolera domeny zostanie przypisana na serwerze z systemem Windows, wartość ustawienia `osProductType` zostaje zmieniona z `server` na `dc`. Takie komputery nie będą uwzględniane w wynikach wyszukiwania `osProductType='server'`. • `'server'` • `'workstation'`		
`osSp`	Dodatek Service Pack systemu operacyjnego.	`osSp = 1`	Tak
`osVersionMajor`	Wersja główna systemu operacyjnego.	`osVersionMajor = 1`	Tak
`osVersionMinor`	Wersja poprawkowa systemu operacyjnego.	`osVersionMinor > 1`	Tak
Agent			
`agentVersion`	Wersja zainstalowanego agenta ochrony.	`agentVersion LIKE '12.0.*'`	Tak
`hostId`	Wewnętrzny identyfikator agenta ochrony. Aby wyświetlić identyfikator agenta ochrony, w obszarze **Urządzenia** wybierz urządzenie, kliknij **Szczegóły** > **Wszystkie właściwości**. Sprawdź wartość `id` właściwości `agent`.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tak
`virtualType`	Typ maszyny wirtualnej. Możliwe wartości:	`virtualType = 'vmwesx'`	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	• `'vmwesx'` Maszyny wirtualne VMware. • `'mshyperv'` Maszyny wirtualne Hyper-V. • `'pcs'` Maszyny wirtualne Virtuozzo. • `'hci'` Maszyny wirtualne Virtuozzo Hybrid Infrastructure. • `'scale'` Maszyny wirtualne Scale Computing HC3. • `'ovirt'` Maszyny wirtualne oVirt		
`insideVm`	Maszyna wirtualna zawierająca agenta. Możliwe wartości: • `true` • `false`	`insideVm = true`	Tak
Lokalizacja			
`tenant`	Nazwa dzierżawcy, w którego obszarze znajduje się urządzenie.	`tenant = 'Unit 1'`	Tak
`tenantId`	Identyfikator dzierżawcy, w którego obszarze znajduje się urządzenie. Aby wyświetlić identyfikator dzierżawcy, w obszarze **Urządzenia** wybierz urządzenie i kliknij **Szczegóły** > **Wszystkie właściwości**. Identyfikator jest pokazywany w polu `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Tak

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
`ou`	Urządzenia należące do wskazanej jednostki organizacyjnej w usłudze Active Directory.	`ou IN ('RnD', 'Computers')`	Tak
Status			
`state`	Stan urządzenia. Możliwe wartości: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	Nie
status	Stan ochrony. Możliwe wartości: • `ok` • `warning` • `error` • `critical` • `protected` • `notProtected`	`status = 'ok'` `status IN ('error', 'warning')`	Nie
`protectedByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze. Aby wyświetlić	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	identyfikator planu, w sekcji **Zarządzanie** > **Plany ochrony** wybierz plan, a następnie kliknij kolejno pasek w kolumnie **Status** i nazwę statusu. Zostanie utworzone nowe wyszukiwanie z identyfikatorem planu.		
`okByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **OK**.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`errorByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **Błąd**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`warningByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **Ostrzeżenie**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`runningByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **Uruchomione**.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`interactionByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **Wymagane działanie**.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`lastBackupTime`*	Data i godzina ostatniego pomyślnego utworzenia kopii zapasowej. Format jest następujący:	`lastBackupTime > '2023-03-11'` `lastBackupTime <= '2023-03-11 00:15'`	Nie

© Acronis International GmbH, 2003-2024

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	`'RRRR-MM-DD GG:MM'`.	`lastBackupTime is null`	
`lastBackupTryTime *`	Godzina ostatniej próby utworzenia kopii zapasowej. Format jest następujący: `'RRRR-MM-DD GG:MM'`.	`lastBackupTryTime >= '2023-03-11'`	Nie
`nextBackupTime*`	Godzina następnego utworzenia kopii zapasowej. Format jest następujący: `'RRRR-MM-DD GG:MM'`.	`nextBackupTime >= '2023-08-11'`	Nie
`lastVAScanTime*`	Data i godzina ostatniej pomyślnej operacji oceny luk w zabezpieczeniach. Format jest następujący: `'RRRR-MM-DD GG:MM'`.	`lastVAScanTime > '2023-03-11' lastVAScanTime <= '2023-03-11 00:15'` `lastVAScanTime is null`	Tak
`lastVAScanTryTime *`	Czas ostatniej próby oceny luk w zabezpieczeniach. Format jest następujący: `'RRRR-MM-DD GG:MM'`.	`lastVAScanTimeTryTime >= '2022-03-11'`	Tak
`nextVAScanTime*`	Czas następnej oceny luk w zabezpieczeniach. Format jest następujący: `'RRRR-MM-DD GG:MM'`.	`nextVAScanTime <= '2023-08-11'`	Tak
`network_status`	Status izolacji sieci w usłudze Endpoint Detection and Response (EDR). Możliwe wartości: • `connected` • `isolated`	`network_status= 'connected'`	Tak

© Acronis International GmbH, 2003-2024

Uwaga

W przypadku pominięcia wartości godziny i minut za czas rozpoczęcia uznaje się RRRRR-MM-DD 00:00, a za czas zakończenia — RRRR-MM-DD 23:59:59. Na przykład `lastBackupTime = 2023-01-20` oznacza, że w wynikach wyszukiwania zostaną uwzględnione wszystkie kopie zapasowe utworzone między
`lastBackupTime >= 2023-01-20 00:00` a `lastBackupTime <= 2023-01-20 23:59:59`.

Operatory wyszukiwania

W poniższej tabeli zestawiono operatory, których można używać w zapytaniach wyszukiwania.

W jednym zapytaniu można użyć kilku operatorów.

Operator	Zastosowanie	Znaczenie	Przykłady
`AND`	Wszystkie obciążenia	Operator iloczynu logicznego	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Wszystkie obciążenia	Operator sumy logicznej	`state = 'backup' OR state = 'interactionRequired'`
`NOT`	Wszystkie obciążenia	Operator negacji logicznej	`NOT(osProductType = 'workstation')`
`IN (<value1>,... <valueN>)`	Wszystkie obciążenia	Ten operator służy do sprawdzania, czy wyrażenie jest zgodne z jakąkolwiek wartością obecną na liście wartości.	`osType IN ('windows', 'linux')`
`NOT IN`	Wszystkie obciążenia	Ten operator jest przeciwieństwem operatora `W`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'wildcard pattern'`	Wszystkie obciążenia	Ten operator służy do sprawdzania, czy wyrażenie pasuje do wzorca z symbolem wieloznacznym.
		Można używać następujących operatorów symboli wieloznacznych:
		• * lub % Gwiazdka i znak procentu
			`name LIKE 'en-00'`
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

© Acronis International GmbH, 2003-2024

Operator	Zastosowanie	Znaczenie	Przykłady
		reprezentują zero, jeden lub wiele znaków • _ Podkreślenie reprezentuje pojedynczy znak	

`NOT LIKE 'wildcard pattern'`	Wszystkie obciążenia	Ten operator jest przeciwieństwem operatora `LIKE`.
		Można używać następujących operatorów symboli wieloznacznych:
		• * lub % Gwiazdka i znak procentu reprezentują zero, jeden lub wiele znaków
		• _ Podkreślenie reprezentuje pojedynczy znak
			`NOT name LIKE 'en-00'`
			`NOT name LIKE '*en-00'`
			`NOT name LIKE '*en-00*'`
			`NOT name LIKE 'en-00_'`

`RANGE (<starting_value>, <ending_value>)`	Wszystkie obciążenia	Ten operator służy do sprawdzania, czy wyrażenie mieści się w przedziale wartości (włącznie).
		W przypadku zapytań wyszukiwania z ciągami alfanumerycznymi stosowana jest kolejność sortowania systemu ASCII, ale nie jest uwzględniana wielkość liter.
			`ip RANGE ('10.250.176.1','10.250.176.50')`
			`name RANGE('a','d')`
			Za pomocą tego zapytania można wyfiltrować wszystkie imiona zaczynające się od A, B i C, na przykład `Agnieszka`, `Beata`, `Cezary`. Jednak tylko jedna litera D spełnia wymagania, więc imiona z większą liczbą liter, na przykład `Dorota` lub `Dariusz` nie zostaną uwzględnione.
			W celu uzyskania tego samego wyniku możesz też użyć następującego zapytania:
			`name >= 'a' AND name <= 'd'`

= lub ==	Wszystkie obciążenia	Operator *Równe*	`osProductType = 'server'`
!= lub <>	Wszystkie obciążenia	Operator *Różne od*	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`

© Acronis International GmbH, 2003-2024

Operator	Zastosowanie	Znaczenie	Przykłady
<	Obciążenia inne niż międzychmurowe	Operator *Mniej niż*	`memorySize < 1024`
>	Obciążenia inne niż międzychmurowe	Operator *Więcej niż*.	`diskSize > 300GB`
<=	Obciążenia inne niż międzychmurowe	Operator *Mniej niż lub równe*	`lastBackupTime <= '2022-03-11 00:15'`
>=	Obciążenia inne niż międzychmurowe	Operator *Więcej niż lub równe*	`nextBackupTime >= '2022-08-11'`

Edytowanie grupy dynamicznej

Grupę dynamiczną można edytować przez zmianę zapytania wyszukiwania, od którego zależy zawartość grupy.

W przypadku grup dynamicznych opartych na usłudze Active Directory można też zmienić grupę usługi Active Directory.

Aby edytować grupę dynamiczną

Przez zmianę zapytania wyszukiwania

1. Kliknij **Urządzenia**, a następnie przejdź do grupy, którą chcesz edytować, i ją zaznacz.
2. Kliknij ikonę koła zębatego obok nazwy grupy, a następnie kliknij **Edytuj**. Możesz też kliknąć **Edytuj** w panelu **Czynności**.
3. Zmień zapytanie wyszukiwania, modyfikując atrybuty wyszukiwania, ich wartości lub operatory wyszukiwania, a następnie kliknij **Szukaj**.
4. Kliknij **Zapisz** obok pola wyszukiwania.

Przez zmianę grupy usługi Active Directory

Uwaga
Ta procedura dotyczy grup dynamicznych opartych na usłudze Active Directory. Grupy dynamiczne oparte na usłudze Active Directory są dostępne tylko w sekcji **Microsoft 365** > **Użytkownicy**.

1. Kliknij **Urządzenia**, przejdź do sekcji **Urządzenia** > **Microsoft 365** > Twoja organizacja > **Użytkownicy**.
2. Wybierz grupę dynamiczną, którą chcesz edytować.
3. Kliknij ikonę koła zębatego obok nazwy grupy, a następnie kliknij **Edytuj**. Możesz też kliknąć **Edytuj** w panelu **Czynności**.
4. Zmień zawartość grupy, wykonując dowolne z następujących czynności:
   - Zmień już wybraną grupę usługi Active Directory: kliknij jej nazwę, a następnie wybierz z otwartej listy nową grupę usługi Active Directory.

© Acronis International GmbH, 2003-2024

- Edytuj zapytanie wyszukiwania i kliknij **Szukaj**.

  Zapytanie wyszukiwania jest ograniczone do aktualnie wybranej grupy Active Directory.

5. Kliknij **Zapisz** obok pola wyszukiwania.

Zmiany edycyjne można też zapisać bez zastępowania bieżącej grupy. Aby zapisać edytowaną konfigurację jako nową grupę, kliknij przycisk strzałki obok pola wyszukiwania, a następnie kliknij **Zapisz jako**.

Usuwanie grupy

Po usunięciu grupy urządzeń wszystkie plany zastosowane do tej grupy zostaną odwołane. Obciążenia należące do tej grupy przestaną być chronione, jeśli nie są do nich zastosowane inne plany.

Aby usunąć grupę urządzeń

1. Kliknij **Urządzenia**, a następnie przejdź do grupy, którą chcesz usunąć.
2. Kliknij ikonę koła zębatego obok nazwy grupy, a następnie kliknij **Usuń**.
3. Potwierdź wybór, klikając **Usuń**.

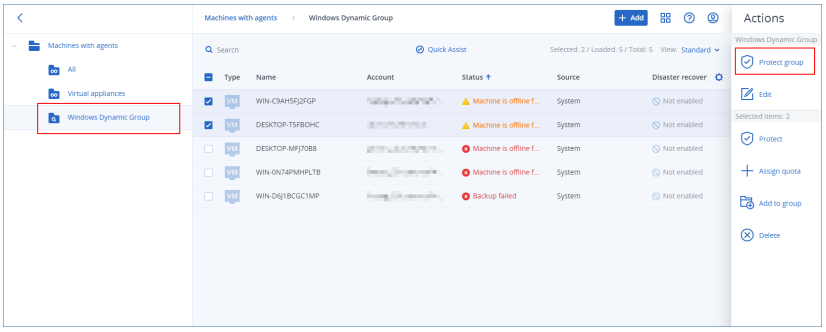
Stosowanie planu do grupy

W celu zastosowania planu do grupy można najpierw wybrać grupę, a następnie przypisać do niej plan.

Ewentualnie można otworzyć plan do edycji, a następnie dodać do niego grupę.

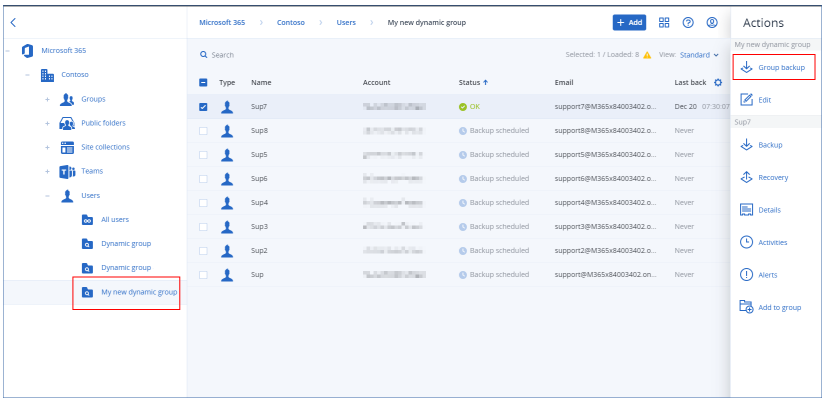
Aby zastosować plan do grupy

1. Kliknij **Urządzenia**, a następnie przejdź do grupy, do której chcesz zastosować plan.
2. [W przypadku obciążeń innych niż międzychmurowe] Kliknij **Chroń grupę**.



   Zostanie wyświetlona lista planów, które można zastosować.
3. [W przypadku obciążeń międzychmurowych] Kliknij **Kopia zapasowa grupy**.

© Acronis International GmbH, 2003-2024



Zostanie wyświetlona lista planów tworzenia kopii zapasowych, które można zastosować.

4. [Aby zastosować już istniejący plan] Wybierz plan, a następnie kliknij **Zastosuj**.
5. [Aby utworzyć nowy plan] Kliknij **Utwórz plan**, wybierz typ planu, a następnie utwórz nowy plan.
   Dodatkowe informacje na temat dostępnych typów planów i instrukcje tworzenia planów można znaleźć w sekcji "Plany obsługiwane w przypadku grup urządzeń" (s. 336).

Uwaga
Plany tworzenia kopii zapasowych stosowane do grup urządzeń międzychmurowych mają automatycznie tworzony harmonogram uruchamiania raz dziennie. Nie można uruchamiać tych planów na żądanie — przez kliknięcie **Uruchom teraz**.

Odwoływanie planu z grupy

W celu odwołania planu z grupy należy najpierw wybrać grupę, a następnie odwołać z niej plan.

Ewentualnie można otworzyć plan do edycji, a następnie usunąć z niego grupę.

Aby odwołać plan z grupy

1. Kliknij **Urządzenia**, a następnie przejdź do grupy, z której chcesz odwołać plan.
2. [W przypadku obciążeń innych niż międzychmurowe] Kliknij **Chroń grupę**.
   Zostanie wyświetlona lista planów zastosowanych do grupy.
3. [W przypadku obciążeń międzychmurowych] Kliknij **Kopia zapasowa grupy**.
   Zostanie wyświetlona lista planów tworzenia kopii zapasowych zastosowanych do grupy.
4. Wybierz plan, który chcesz odwołać.
5. [W przypadku obciążeń innych niż międzychmurowe] Kliknij ikonę wielokropka (...), a następnie kliknij **Odwołaj**.
6. [W przypadku obciążeń międzychmurowych] Kliknij ikonę koła zębatego, a następnie kliknij **Odwołaj**.

© Acronis International GmbH, 2003-2024

Korzystanie z modułu kontroli urządzeń

Będąc elementem planów ochrony usługi Cyber Protection, moduł kontroli urządzeń[1] na każdym komputerze korzysta z funkcji agenta dla rozwiązania Data Loss Prevention[2] w celu wykrywania oraz blokowania nieuprawnionego dostępu do danych i ich przesyłania za pośrednictwem kanałów komputera lokalnego. Zapewnia on precyzyjną kontrolę nad szeroką gamą ścieżek wycieku danych, w tym nad wymianą danych przy użyciu nośników wymiennych, drukarek, urządzeń wirtualnych i przekierowanych oraz schowka systemu Windows.

Moduł ten jest dostępny w edycjach Cyber Protect Essentials, Cyber Protect Standard i Cyber Protect Advanced, które są licencjonowane według obciążeń.

Uwaga
W przypadku komputerów z systemem Windows funkcje kontroli urządzeń wymagają zainstalowania agenta dla rozwiązania Data Loss Prevention. Zostanie on zainstalowany automatycznie w przypadku chronionych obciążeń, jeśli w ich planach ochrony jest włączony moduł **Kontrola urządzeń**.

Moduł kontroli urządzeń korzysta z funkcji ochrony przed utratą danych[3] agenta w celu wymuszenia kontekstowej kontroli nad operacjami uzyskiwania dostępu do danych i ich przesyłania na chronionym komputerze. Obejmują one dostęp użytkownika do urządzeń peryferyjnych i portów, drukowanie dokumentów, operacje kopiowania/wklejania przy użyciu schowka, operacje formatowania i wysuwania nośników, a także synchronizację z lokalnie podłączonymi urządzeniami mobilnymi. Agent dla rozwiązania Data Loss Prevention obejmuje środowisko dla wszystkich komponentów centralnego zarządzania i administracji modułu kontroli urządzeń, w związku z czym musi zostać zainstalowany na każdym komputerze, który ma być chroniony za pomocą tego modułu. Agent zezwala na czynności użytkownika, ogranicza je lub odmawia ich wykonania na

[1]Będąc elementem planu ochrony, moduł kontroli urządzeń na każdym komputerze korzysta z funkcji agenta ochrony przed utratą danych w celu wykrywania oraz blokowania nieuprawnionego dostępu do danych i ich przesyłania za pośrednictwem kanałów komputera lokalnego. Obejmują one dostęp użytkownika do urządzeń peryferyjnych i portów, drukowanie dokumentów, operacje kopiowania/wklejania przy użyciu schowka, operacje formatowania i wysuwania nośników, a także synchronizację z lokalnie podłączonymi urządzeniami mobilnymi. Moduł kontroli urządzeń zapewnia granularną, kontekstową kontrolę nad typami urządzeń i portami, do których użytkownicy mają dostęp na chronionym komputerze, oraz nad działaniami, które użytkownicy mogą podejmować na tych urządzeniach.
[2]Komponent kliencki systemu ochrony przed utratą danych, który chroni hosta przed nieuprawnionym wykorzystywaniem, przesyłaniem i przechowywaniem poufnych, chronionych lub wrażliwych danych dzięki zastosowaniu kombinacji technik analizy kontekstu i zawartości oraz egzekwowanie centralnie zarządzanych zasad ochrony przed utratą danych. Rozwiązanie Cyber Protection udostępnia w pełni funkcjonalnego agenta ochrony przed utratą danych. Funkcjonalność tego agenta na chronionym komputerze jest jednak ograniczona do zestawu funkcji ochrony przed utratą danych dostępnych na potrzeby licencjonowania rozwiązania Cyber Protection i zależy od planu ochrony zastosowanego do tego komputera.
[3]System zintegrowanych technologii oraz środków organizacyjnych mających na celu wykrywanie i blokowanie przypadkowego bądź celowego ujawniania poufnych, chronionych lub wrażliwych danych albo uzyskiwania do nich dostępu przez nieuprawnione podmioty z zewnątrz lub wewnątrz organizacji, a także przekazywania takich danych do niezaufanych środowisk.

© Acronis International GmbH, 2003-2024

podstawie ustawień kontroli urządzeń otrzymanych z planu ochrony zastosowanego do chronionego komputera.

Moduł kontroli urządzeń kontroluje dostęp do różnych urządzeń peryferyjnych, używanych bezpośrednio na chronionych komputerach lub przekierowanych w środowiskach wirtualizacji hostowanych na chronionych komputerach. Rozpoznaje on przekierowane urządzenia w środowiskach Microsoft Remote Desktop Server, Citrix XenDesktop / XenApp / XenServer i VMware Horizon. Może też kontrolować operacje kopiowania danych między schowkiem systemu operacyjnego gościa działającego na urządzeniu VMware Workstation / Player, Oracle VM VirtualBox lub Windows Virtual PC a schowkiem systemu operacyjnego hosta działającego na chronionym komputerze.

Moduł kontroli urządzeń może chronić komputery z następującymi systemami operacyjnymi:

Kontrola urządzeń

- Microsoft Windows 7 Service Pack 1 lub nowszy
- Microsoft Windows Server 2008 R2 lub nowszy
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

Uwaga
Agent dla usługi Zapobieganie utracie danych przeznaczony dla systemu macOS obsługuje tylko procesory x64. Procesory Apple Silicon oparte na architekturze ARM nie są obsługiwane.

Zapobieganie utracie danych

- Microsoft Windows 7 Service Pack 1 lub nowszy
- Microsoft Windows Server 2008 R2 lub nowszy

Uwaga
Agenta dla usługi Zapobieganie utracie danych można instalować w nieobsługiwanych systemach macOS, ponieważ jest integralną częścią programu agenta dla systemu Mac. W takim przypadku w konsoli usługi Cyber Protect pojawi się informacja, że agent dla usługi Zapobieganie utracie danych jest zainstalowany na komputerze, ale funkcje kontroli urządzeń i zapobiegania utracie danych nie będą działać. Funkcja kontroli urządzeń będzie działać tylko w systemach macOS obsługiwanych przez agenta dla usługi Zapobieganie utracie danych.

Ograniczenia dotyczące używania agenta dla rozwiązania Data Loss Prevention w środowiskach Hyper-V

Nie instaluj agenta dla rozwiązania Data Loss Prevention na hostach Hyper-V w klastrach Hyper-V, ponieważ może on powodować problemy objawiające się niebieskim ekranem, głównie w klastrach

© Acronis International GmbH, 2003-2024

Hyper-V z klastrowanymi woluminami udostępnionymi.

W przypadku używania którejkolwiek z poniższych wersji agenta dla Hyper-V trzeba ręcznie usunąć agenta dla rozwiązania Data Loss Prevention:

- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

Aby usunąć agenta dla rozwiązania Data Loss Prevention, ręcznie uruchom instalator na hoście Hyper-V i wyczyść pole wyboru Agent dla rozwiązania Data Loss Prevention lub uruchom następujące polecenie:

```
<installer_name> --remove-components=agentForDlp -quiet
```

Moduł kontroli urządzeń można włączyć i skonfigurować w sekcji **Kontrola urządzeń** planu ochrony w konsoli Cyber Protect. Wskazówki na ten temat można znaleźć w instrukcji włączania lub wyłączania kontroli urządzeń.

W sekcji **Kontrola urządzeń** wyświetlane jest podsumowanie konfiguracji modułu:

- Ustawienia dostępu — zawiera zestawienie typów urządzeń i portów z ograniczonym dostępem (odmowa lub tylko do odczytu), jeśli takie typy i porty występują. W przeciwnym razie zawiera wszystkie dozwolone typy urządzeń. Kliknij to zestawienie, aby wyświetlić lub zmienić ustawienia dostępu (zobacz instrukcję wyświetlania lub zmieniania ustawień dostępu).
- Lista dozwolonych typów urządzeń — wskazuje, ile podklas urządzeń jest dozwolonych przez wykluczenie z kontroli dostępu do urządzeń, jeśli takie klasy występują. W przeciwnym razie wskazuje, że lista dozwolonych jest pusta. Kliknij to zestawienie, aby wyświetlić lub zmienić wybór dozwolonych podklas urządzeń (zobacz instrukcję wykluczania podklas z kontroli dostępu).

© Acronis International GmbH, 2003-2024

- Lista dozwolonych urządzeń USB — wskazuje, ile urządzeń USB lub ich modeli jest dozwolonych przez wykluczenie z kontroli dostępu do urządzeń, jeśli takie urządzenia występują. W przeciwnym razie wskazuje, że lista dozwolonych jest pusta. Kliknij to zestawienie, aby wyświetlić lub zmienić listę dozwolonych urządzeń USB lub ich modeli (zobacz instrukcję wykluczania wybranych urządzeń USB z kontroli dostępu).
- Wykluczenia — umożliwia wyświetlenie, ile wykluczeń kontroli dostępu zostało ustawionych w przypadku schowka systemu Windows, rejestratorów zrzutów ekranu, drukarek i urządzeń mobilnych.

Korzystanie z kontroli urządzeń

Ta sekcja zawiera instrukcje krok po kroku dotyczące podstawowych zadań wykonywanych podczas korzystania z modułu kontroli urządzeń.

Włączanie lub wyłączanie kontroli urządzeń

Podczas tworzenia planu ochrony można wyłączyć kontrolę urządzeń. Można też zmienić istniejący już plan ochrony w celu włączenia lub wyłączenia kontroli urządzeń.

Aby włączyć lub wyłączyć kontrolę urządzeń

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wykonaj jedną z następujących czynności, aby otworzyć panel planu ochrony:
   - Jeśli chcesz utworzyć nowy plan ochrony, wybierz komputer, który ma być chroniony, a następnie kliknij **Chroń** i **Utwórz plan**.
   - Jeśli chcesz zmienić już istniejący plan ochrony, wybierz chroniony komputer, kliknij **Chroń**, kliknij wielokropek (...) obok nazwy planu ochrony, a następnie kliknij **Edytuj**.
3. Na panelu planu ochrony przejdź do obszaru **Kontrola urządzeń** i włącz lub wyłącz przełącznik **Kontrola urządzeń**.
4. Aby zastosować wprowadzone zmiany, wykonaj jedną z następujących czynności:
   - W przypadku tworzenia planu kliknij **Utwórz**.
   - W przypadku edytowania planu kliknij **Zapisz**.

Panel planu ochrony można też otworzyć z poziomu karty Zarządzanie.Funkcja ta jednak jest niedostępna w niektórych wersjach usługi Cyber Protection.

Umożliwianie korzystania z modułu kontroli urządzeń w systemie macOS

Ustawienia kontroli urządzeń w planie ochrony zaczynają obowiązywać dopiero po załadowaniu sterownika kontroli urządzeń w ramach chronionego obciążenia. W tej sekcji opisano, jak załadować sterownik kontroli urządzeń, aby umożliwić korzystanie z modułu kontroli urządzeń w systemie macOS. Jest to operacja jednorazowa, która wymaga uprawnień administratora na komputerze końcowym.

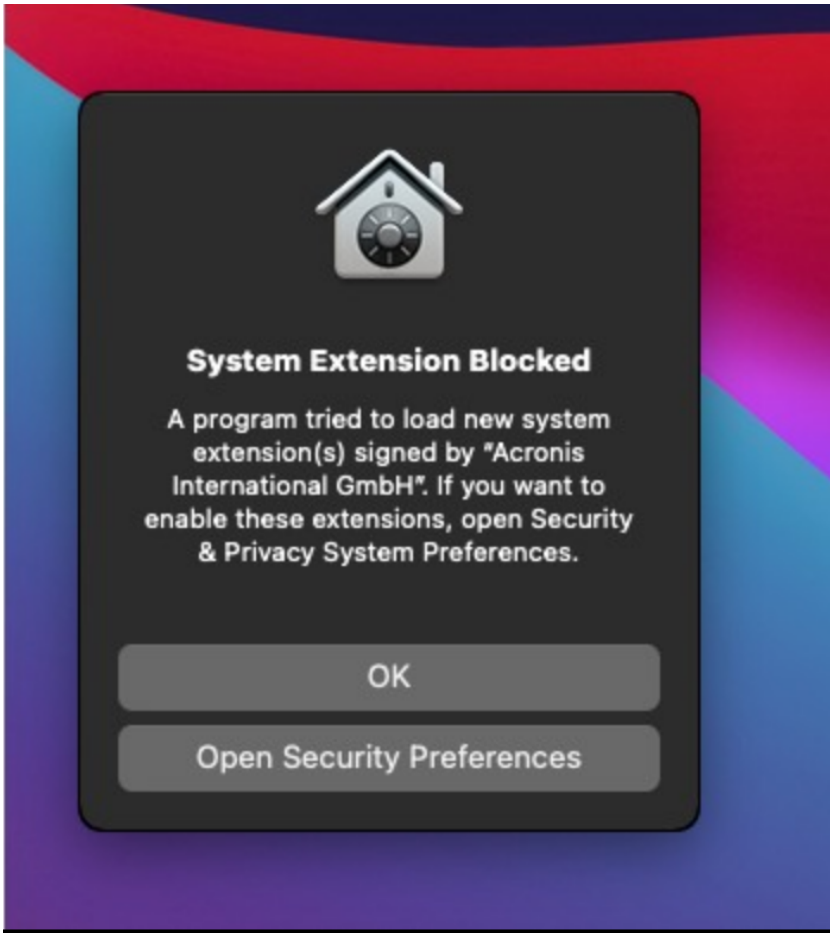
Obsługiwane wersje systemu macOS:

© Acronis International GmbH, 2003-2024

- macOS 10.15 (Catalina) i nowsze
- macOS 11.2.3 (Big Sur) i nowsze
- macOS 12.2 (Monterey) i nowsze
- macOS 13.2 (Ventura) i nowsze

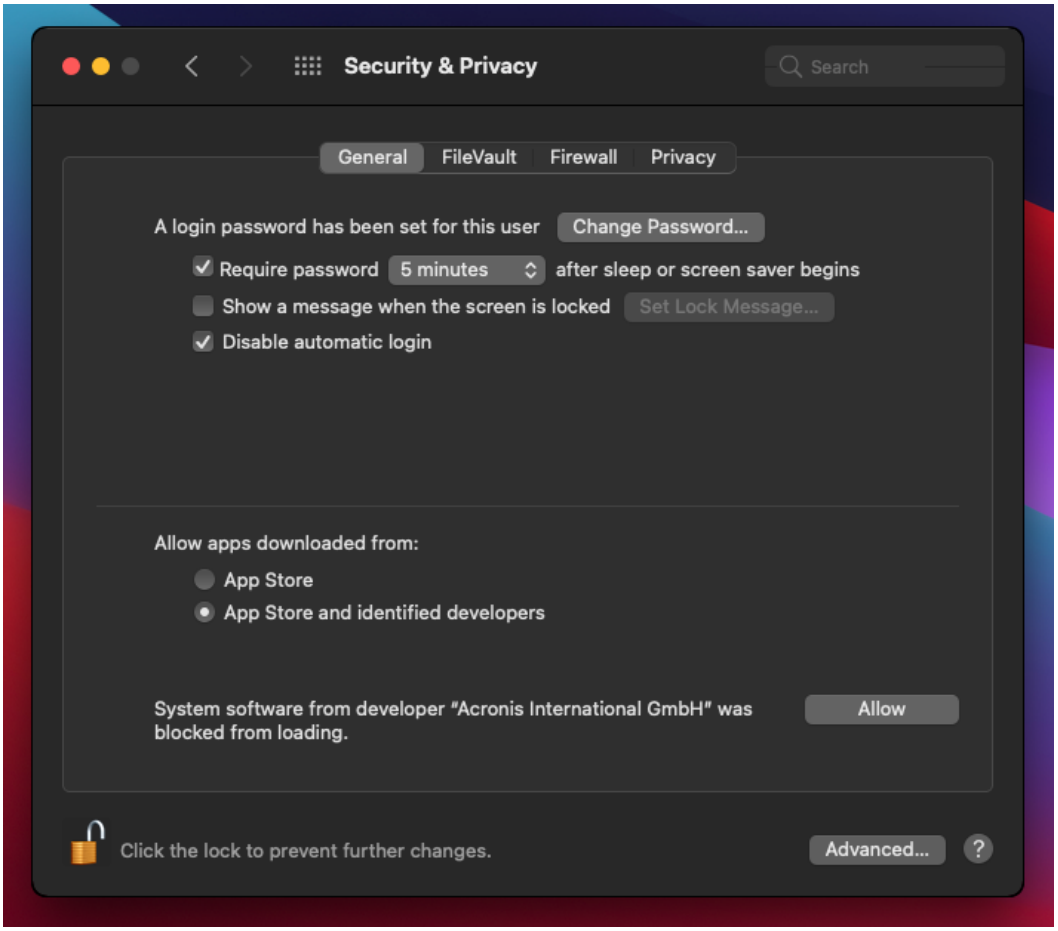
Aby umożliwić korzystanie z modułu kontroli urządzeń w systemie macOS

1. Zainstaluj agenta dla systemu Mac na komputerze, który chcesz chronić.
2. W planie ochrony włącz ustawienia kontroli urządzeń.
3. Zastosuj plan ochrony.
4. W przypadku chronionego obciążenia pojawi się ostrzeżenie „Rozszerzenie systemu zablokowane”. Kliknij **Otwórz preferencje zabezpieczeń**.



© Acronis International GmbH, 2003-2024

5. W wyświetlonym okienku **Bezpieczeństwo i prywatność** zaznacz **App Store i od zidentyfikowanych autorów** i kliknij **Zezwól**.



6. W wyświetlonym oknie dialogowym kliknij **Uruchom ponownie**, aby uruchomić ponownie obciążenie i aktywować ustawienia kontroli urządzeń.

Uwaga
Jeśli ustawienia kontroli urządzeń zostaną wyłączone, a następnie ponownie włączone, nie trzeba powtarzać tych czynności.

Wyświetlanie lub zmienianie ustawień dostępu

Na panelu planu ochrony możesz zarządzać ustawieniami dostępu do modułu kontroli urządzeń. W ten sposób możesz zezwolić na dostęp lub odmówić dostępu do określonych typów urządzeń, a także włączyć lub wyłączyć powiadomienia i alerty.

Aby wyświetlić lub zmienić ustawienia dostępu

1. Otwórz panel odpowiedniego planu ochrony i włącz w tym planie kontrolę urządzeń (zobacz instrukcję włączania lub wyłączania kontroli urządzeń).
2. Kliknij ikonę strzałki obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij łącze obok pozycji **Ustawienia dostępu**.

© Acronis International GmbH, 2003-2024

3. Na wyświetlonej stronie zarządzania ustawieniami dostępu wyświetl lub zmień ustawienia dostępu stosownie do potrzeb.

Uwaga
Ustawienia dostępu skonfigurowane w funkcji Kontrola urządzeń mogą zostać zastąpione w przypadku chronienia obciążenia przy użyciu zarówno funkcji Kontrola urządzeń, jak i modułu Advanced DLP. Zobacz "Włączanie modułu Advanced Data Loss Prevention w planach ochrony" (s. 938).

Włączanie lub wyłączanie powiadomień systemu operacyjnego i alertów usługi

Podczas zarządzania ustawieniami dostępu można włączać i wyłączać powiadomienia systemu operacyjnego i alerty usługi informujące o próbach wykonania przez użytkownika niedozwolonej czynności.

Aby włączyć lub wyłączyć powiadomienia systemu operacyjnego

1. Postąp zgodnie z instrukcją wyświetlania lub zmieniania ustawień dostępu.
2. Na stronie zarządzania ustawieniami dostępu zaznacz lub wyczyść pole wyboru **Pokazuj powiadomienia systemu operacyjnego, jeśli użytkownicy spróbują użyć zablokowanego typu urządzenia lub portu**.

Aby włączyć lub wyłączyć alerty usługi

1. Postąp zgodnie z instrukcją wyświetlania lub zmieniania ustawień dostępu.
2. Na stronie zarządzania ustawieniami dostępu zaznacz lub wyczyść pole wyboru **Pokaż alert** przy odpowiednich typach urządzeń.

Pole wyboru **Pokaż alert** jest dostępne tylko w przypadku typów urządzeń z ograniczonym dostępem (Tylko do odczytu lub Odmowa dostępu), z wyjątkiem rejestratorów zrzutów ekranu.

Wykluczanie podklas urządzeń z kontroli dostępu

Na panelu planu ochrony wybierz podklasy urządzeń, które mają być wykluczone z kontroli dostępu. W wyniku takich ustawień dostęp do tych urządzeń będzie dozwolony niezależnie od ustawień dostępu do kontroli urządzeń.

Aby wykluczyć podklasy urządzeń z kontroli dostępu

1. Otwórz panel odpowiedniego planu ochrony i włącz w tym planie kontrolę urządzeń (zobacz instrukcję włączania lub wyłączania kontroli urządzeń).
2. Kliknij ikonę strzałki obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij łącze obok pozycji **Lista dozwolonych typów urządzeń**.
3. Na wyświetlonej stronie zarządzania listą dozwolonych wyświetl lub zmień wybór podklas urządzeń, które mają zostać wykluczone z kontroli dostępu.

© Acronis International GmbH, 2003-2024

Wykluczanie poszczególnych urządzeń USB z kontroli dostępu

Na panelu planu ochrony można wskazać określone urządzenia USB lub modele urządzeń USB, które mają być wykluczone z kontroli dostępu. W wyniku takich ustawień dostęp do tych urządzeń będzie dozwolony niezależnie od ustawień dostępu do kontroli urządzeń.

Aby wykluczyć poszczególne urządzenia USB z kontroli dostępu

1. Otwórz panel odpowiedniego planu ochrony i włącz w tym planie kontrolę urządzeń (zobacz instrukcję włączania lub wyłączania kontroli urządzeń).
2. Kliknij ikonę strzałki obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij łącze obok pozycji **Lista dozwolonych urządzeń USB**.
3. Na wyświetlonej stronie zarządzania listą dozwolonych kliknij **Dodaj z bazy danych**.
4. Na wyświetlonej stronie wybierania urządzeń USB wybierz odpowiednie urządzenia spośród tych, które są zarejestrowane w bazie danych urządzeń USB.
5. Kliknij **Dodaj do listy dozwolonych**.

Aby zatrzymać wykluczenie wybranego urządzenia USB z kontroli dostępu

1. Otwórz panel odpowiedniego planu ochrony i włącz w tym planie kontrolę urządzeń (zobacz instrukcję włączania lub wyłączania kontroli urządzeń).
2. Kliknij ikonę strzałki obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij łącze obok pozycji **Lista dozwolonych urządzeń USB**.
3. Na wyświetlonej stronie zarządzania listą dozwolonych kliknij ikonę usuwania na końcu pozycji listy reprezentującej dane urządzenie USB.

Dodawanie lub usuwanie urządzeń USB w ramach bazy danych

Aby wykluczyć dane urządzenie USB z kontroli dostępu, trzeba je dodać do bazy danych urządzeń USB. Następnie można dodać urządzenia do listy dozwolonych, wybierając je z tej bazy danych.

Poniższe procedury dotyczą planów ochrony z włączoną funkcją kontroli urządzeń.

Aby dodać urządzenia USB do bazy danych

1. Otwórz plan ochrony urządzenia do edycji:
   Kliknij wielokropek (...) widoczny obok nazwy planu ochrony i wybierz **Edytuj**.

   Uwaga
   Aby można było uzyskać dostęp do ustawień kontroli nad urządzeniami, w planie musi być włączona funkcja Kontrola urządzeń.

2. Kliknij ikonę strzałki obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij łącze obok pozycji **Lista dozwolonych urządzeń USB**.
3. Na wyświetlonej stronie **listy dozwolonych urządzeń USB** kliknij **Dodaj z bazy danych**.
4. Na wyświetlonej stronie zarządzania bazą danych urządzeń USB kliknij **Dodaj z bazy danych**.

© Acronis International GmbH, 2003-2024

5. W wyświetlonym oknie dialogowym **Dodaj urządzenie USB** kliknij komputer, do którego jest podłączone dane urządzenie USB.
   Na liście komputerów są wyświetlane tylko komputery działające w trybie online.
   Lista urządzeń USB jest wyświetlana tylko w przypadku komputerów z zainstalowanym agentem do ochrony przed utratą danych.
   Urządzenia USB są wyświetlane w widoku drzewa. Pierwszy poziom drzewa reprezentuje model urządzenia. Drugi poziom reprezentuje konkretne urządzenie danego modelu.
   Niebieska ikona obok opisu urządzenia oznacza, że jest ono aktualnie podłączone do komputera. Jeśli urządzenie nie jest podłączone do komputera, ta ikona jest wyszarzona.
6. Zaznacz pola wyboru odpowiadające urządzeniom USB, które mają zostać dodane do bazy danych, a następnie kliknij **Dodaj do bazy danych**.
   Wybrane urządzenia USB zostaną dodane do bazy danych.
7. Zamknij i zapisz plan ochrony.

Aby dodać urządzenia USB do bazy danych przy użyciu panelu Szczegóły komputera

Uwaga
Ta procedura dotyczy tylko urządzeń, które działają w trybie online i mają zainstalowanego agenta do ochrony przed utratą danych. Nie można wyświetlić listy urządzeń USB w przypadku komputera, który działa w trybie offline lub nie ma zainstalowanego agenta do ochrony przed utratą danych.

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputer, do którego kiedykolwiek było podłączone wybrane urządzenie USB, a następnie w menu po prawej stronie kliknij **Inwentaryzacja**.
   Zostanie otwarty panel szczegółów komputera.
3. Na panelu szczegółów komputera kliknij kartę **Urządzenia USB**.
   Zostanie otwarta lista urządzeń USB znanych na wybranym komputerze.
   Urządzenia USB są wyświetlane w widoku drzewa. Pierwszy poziom drzewa reprezentuje model urządzenia. Drugi poziom reprezentuje konkretne urządzenie danego modelu.
   Niebieska ikona obok opisu urządzenia oznacza, że jest ono aktualnie podłączone do komputera. Jeśli urządzenie nie jest podłączone do komputera, ta ikona jest wyszarzona.
4. Zaznacz pola wyboru odpowiadające urządzeniom USB, które mają zostać dodane do bazy danych, i kliknij **Dodaj do bazy danych**.

Aby dodać urządzenia USB do bazy danych z poziomu alertów usługi

1. W konsoli Cyber Protect przejdź do sekcji **Monitorowanie** > **Alerty**.
2. Znajdź alert związanych z kontrolą urządzeń zawierający informację o odmowie dostępu do danego urządzenia USB.
3. W widoku prostym alertu kliknij **Zezwól na to urządzenie USB**.
   Spowoduje to wykluczenie urządzenia USB z kontroli dostępu i dodanie go do bazy danych na potrzeby przyszłych działań.

Aby dodać urządzenia USB przez zaimportowanie listy urządzeń do bazy danych

© Acronis International GmbH, 2003-2024

Do bazy danych można zaimportować plik JSON z listą urządzeń USB. Zobacz "Importowanie listy urządzeń USB do bazy danych" (s. 380).

Aby usunąć urządzenie USB z bazy danych

1. Otwórz plan ochrony urządzenia do edycji:
   Kliknij wielokropek (...) widoczny obok nazwy planu ochrony i wybierz **Edytuj**.

   Uwaga
   Aby można było uzyskać dostęp do ustawień kontroli nad urządzeniami, w planie musi być włączona funkcja Kontrola urządzeń.

2. Kliknij strzałkę obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij wiersz **Lista dozwolonych urządzeń USB**.
3. Na wyświetlonej stronie zarządzania listą dozwolonych kliknij **Dodaj z bazy danych**.
4. Na stronie wybierania urządzeń USB z bazy danych kliknij wielokropek (...) na końcu pozycji listy reprezentującej urządzenie, kliknij **Usuń** i potwierdź usunięcie.
   Urządzenia USB zostaną usunięte z bazy danych.
5. Zamknij i zapisz plan ochrony.

Wyświetlanie alertów związanych z kontrolą urządzeń

Moduł kontroli urządzeń można skonfigurować tak, aby uruchamiał alerty informujące o odmowie dostępu w przypadku podjęcia przez użytkownika próby użycia określonych typów urządzeń (zobacz Włączanie lub wyłączanie powiadomień systemu operacyjnego i alertów usługi). Aby wyświetlić te alerty, wykonaj niżej opisane czynności.

Aby wyświetlić alerty związane z kontrolą urządzeń

1. W konsoli Cyber Protect przejdź do sekcji **Monitorowanie** > **Alerty**.
2. Poszukaj alertów z następującym statusem:„Zablokowano dostęp do urządzeń peryferyjnych”.

Dodatkowe informacje można znaleźć w sekcji Alerty związane z kontrolą urządzeń.

Ustawienia dostępu

Na stronie **Ustawienia dostępu** można zezwolić na dostęp lub odmówić dostępu do urządzeń określonego typu, a także włączyć lub wyłączyć powiadomienia systemu operacyjnego i alerty związane z kontrolą urządzeń.

Uwaga
Ustawienia dostępu skonfigurowane w funkcji Kontrola urządzeń mogą zostać zastąpione w przypadku chronienia obciążenia przy użyciu zarówno funkcji Kontrola urządzeń, jak i modułu Advanced DLP. Zobacz "Włączanie modułu Advanced Data Loss Prevention w planach ochrony" (s. 938).

© Acronis International GmbH, 2003-2024

Ustawienia dostępu umożliwiają ograniczenie dostępu użytkowników do następujących typów urządzeń i portów:

- **Wymienny** (kontrola dostępu według typów urządzeń) — urządzenia z dowolnym interfejsem do połączeń z komputerem (USB, FireWire, PCMCIA, IDE, SATA, SCSI itd.) rozpoznawane przez system operacyjny jako wymienne urządzenia pamięci masowej (np. dyski flash USB, czytniki kart, napędy magnetooptyczne itd.). Funkcja kontroli urządzeń klasyfikuje wszystkie dyski twarde podłączone przez USB, FireWire i PCMCIA jako urządzenia wymienne. Klasyfikuje jako urządzenia wymienne również niektóre dyski twarde (zazwyczaj SATA i SCSI), jeśli obsługują funkcję „podłączania na gorąco" i nie mają zainstalowanego działającego systemu operacyjnego.

  Możesz zezwolić na pełny dostęp, zezwolić na dostęp tylko do odczytu lub odmówić dostępu do urządzeń wymiennych w celu kontrolowania operacji kopiowania danych na dowolne urządzenie wymienne bądź z dowolnego urządzenia wymiennego w przypadku chronionego komputera. Prawa dostępu nie mają wpływu na urządzenia zaszyfrowane za pomocą funkcji BitLocker lub FileVault (tylko w systemie plików HFS+).

  Ten typ urządzeń jest obsługiwany zarówno w systemie Windows, jak i macOS.
- **Zaszyfrowane urządzenie wymienne** (kontrola dostępu według typów urządzeń) — urządzenia wymienne zaszyfrowane za pomocą funkcji szyfrowania dysków BitLocker (w systemie Windows) lub FileVault (w systemie macOS).

  W systemie macOS są obsługiwane tylko zaszyfrowane dyski wymienne korzystające z systemu plików HFS+ (znanego również jako HFS Plus, Mac OS Extended lub HFS Extended). Zaszyfrowane dyski wymienne korzystające z systemu plików APFS są traktowane jak zwykłe dyski wymienne.

  Możesz zezwolić na pełny dostęp, zezwolić na dostęp tylko do odczytu lub odmówić dostępu do zaszyfrowanych urządzeń wymiennych w celu kontrolowania operacji kopiowania danych na dowolne zaszyfrowane urządzenie wymienne bądź z dowolnego zaszyfrowanego urządzenia wymiennego w przypadku chronionego komputera. Prawa dostępu mają wpływ wyłącznie na urządzenia zaszyfrowane za pomocą funkcji BitLocker lub FileVault (tylko w systemie plików HFS+).

  Ten typ urządzeń jest obsługiwany zarówno w systemie Windows, jak i macOS.
- **Drukarki** (kontrola dostępu według typów urządzeń) — drukarki fizyczne z dowolnym interfejsem do połączeń z komputerem (USB, LPT, Bluetooth itp.), a także drukarki dostępne z komputera w sieci.

  Możesz zezwolić na dostęp lub odmówić dostępu do drukarek w celu kontrolowania drukowania dokumentów na dowolnej drukarce w przypadku chronionego komputera.

  Uwaga
  Po zmianie ustawienia dostępu w przypadku drukarek na **Odmów** trzeba uruchomić ponownie aplikacje i procesy uzyskujące dostęp do drukarek w celu uwzględnienia nowo skonfigurowanych ustawień dostępu. Aby ustawienia dostępu były poprawnie egzekwowane, należy uruchomić ponownie chronione obciążenia.

  Ten typ urządzeń jest obsługiwany tylko w systemie Windows.
- **Schowek** (kontrola dostępu według typów urządzeń) — schowek systemu Windows.

© Acronis International GmbH, 2003-2024

Możesz zezwolić na dostęp lub odmówić dostępu do schowka w celu kontrolowania operacji kopiowania i wklejania danych przez schowek systemu Windows na chronionym komputerze.

Uwaga
Po zmianie ustawienia dostępu w przypadku schowka na **Odmów** trzeba uruchomić ponownie aplikacje i procesy uzyskujące dostęp do schowka w celu uwzględnienia nowo skonfigurowanych ustawień dostępu. Aby ustawienia dostępu były poprawnie egzekwowane, należy uruchomić ponownie chronione obciążenia.

Ten typ urządzeń jest obsługiwany tylko w systemie Windows.

- **Rejestrator zrzutów ekranu** (kontrola dostępu według typów urządzeń) — umożliwia rejestrowanie zrzutów ekranu całego ekranu, aktywnego okna lub wybranego fragmentu ekranu.
  Możesz zezwolić na dostęp lub odmówić dostępu do rejestratora zrzutów ekranu, aby kontrolować rejestrowanie zrzutów ekranu na chronionym komputerze.

  Uwaga
  Po zmianie ustawienia dostępu w przypadku rejestratora zrzutów ekranu na **Odmów** trzeba uruchomić ponownie aplikacje i procesy uzyskujące dostęp do rejestratora zrzutów ekranu w celu uwzględnienia nowo skonfigurowanych ustawień dostępu. Aby ustawienia dostępu były poprawnie egzekwowane, należy uruchomić ponownie chronione obciążenia.

  Ten typ urządzeń jest obsługiwany tylko w systemie Windows.
- **Urządzenia mobilne** (kontrola dostępu według typów urządzeń) — urządzenia (takie jak smartfony z systemem Android itp.), które komunikują się z komputerem przy użyciu protokołu Media Transfer Protocol (MTP) i mają dowolny interfejs do połączeń z komputerem (USB, IP, Bluetooth).
  Możesz zezwolić na pełny dostęp, zezwolić na dostęp tylko do odczytu lub odmówić dostępu do urządzeń mobilnych w celu kontrolowania operacji kopiowania danych na dowolne urządzenie mobilne bądź z dowolnego urządzenia mobilnego przy użyciu protokołu MTP w przypadku chronionego komputera.

  Uwaga
  Po zmianie ustawienia dostępu w przypadku urządzeń mobilnych na **Tylko do odczytu** lub **Odmów** trzeba uruchomić ponownie aplikacje i procesy uzyskujące dostęp do urządzeń mobilnych w celu uwzględnienia nowo skonfigurowanych ustawień dostępu. Aby ustawienia dostępu były poprawnie egzekwowane, należy uruchomić ponownie chronione obciążenia.

  Ten typ urządzeń jest obsługiwany tylko w systemie Windows.
- **Bluetooth** (kontrola dostępu według typów urządzeń) — zewnętrzne i wewnętrzne urządzenia Bluetooth z dowolnym interfejsem do połączeń z komputerem (USB, PCMCIA itp.). To ustawienie pozwala kontrolować korzystanie z urządzeń tego typu, a nie wymianę danych za ich pomocą.
  Możesz zezwolić na dostęp do łączności Bluetooth lub odmówić takiego dostępu w celu kontrolowania korzystania z urządzeń Bluetooth na chronionym komputerze.

© Acronis International GmbH, 2003-2024

Uwaga

W systemie macOS prawa dostępu dotyczące łączności Bluetooth nie mają wpływu na urządzenia Bluetooth HID. Dostęp do tych urządzeń jest zawsze dozwolony, aby zapobiec wyłączeniu bezprzewodowych urządzeń HID (mysz i klawiatur) na komputerach iMac i Mac Pro.

Ten typ urządzeń jest obsługiwany zarówno w systemie Windows, jak i macOS.

- **Dyski optyczne** (kontrola dostępu według typów urządzeń) — zewnętrzne i wewnętrzne napędy CD/DVD/BD (w tym nagrywarki) z dowolnym interfejsem do połączeń z komputerem (IDE, SATA, USB, FireWire, PCMCIA itp.).

  Możesz zezwolić na pełny dostęp, zezwolić na dostęp tylko do odczytu lub odmówić dostępu do napędów optycznych w celu kontrolowania operacji kopiowania danych na dowolny napęd optyczny bądź z dowolnego napędu optycznego w przypadku chronionego komputera.

  Ten typ urządzeń jest obsługiwany zarówno w systemie Windows, jak i macOS.
- **Stacje dyskietek** (kontrola dostępu według typów urządzeń) — zewnętrzne i wewnętrzne stacje dyskietek z dowolnym interfejsem do połączeń z komputerem (IDE, USB, PCMCIA itp.). Niektóre modele stacji dyskietek są rozpoznawane przez system operacyjny jako dyski wymienne, a wówczas funkcja kontroli urządzeń również rozpoznaje je jako urządzenia wymienne.

  Możesz zezwolić na pełny dostęp, zezwolić na dostęp tylko do odczytu lub odmówić dostępu do stacji dyskietek w celu kontrolowania operacji kopiowania danych na dowolną stację dyskietek bądź z dowolnej stacji dyskietek w przypadku chronionego komputera.

  Ten typ urządzeń jest obsługiwany tylko w systemie Windows.
- **USB** (kontrola dostępu według interfejsów urządzeń) — wszystkie urządzenia podłączane do portu USB, z wyjątkiem koncentratorów.

  Możesz zezwolić na pełny dostęp, zezwolić na dostęp tylko do odczytu lub odmówić dostępu do portu USB w celu kontrolowania operacji kopiowania danych na urządzenia podłączane do dowolnego portu USB bądź z takich urządzeń w przypadku chronionego komputera.

  Ten typ urządzeń jest obsługiwany zarówno w systemie Windows, jak i macOS.
- **FireWire** (kontrola dostępu według interfejsów urządzeń) — wszystkie urządzenia podłączane do portu FireWire (IEEE 1394), z wyjątkiem koncentratorów.

  Możesz zezwolić na pełny dostęp, zezwolić na dostęp tylko do odczytu lub odmówić dostępu do portu FireWire w celu kontrolowania operacji kopiowania danych na urządzenia podłączane do dowolnego portu FireWire bądź z takich urządzeń w przypadku chronionego komputera.

  Ten typ urządzeń jest obsługiwany zarówno w systemie Windows, jak i macOS.
- **Przekierowywane urządzenia** (kontrola dostępu według interfejsów urządzeń) — zamapowane dyski (twarde, wymienne i optyczne), urządzenia USB oraz schowek przekierowywane do wirtualnych sesji aplikacji/pulpitu.

  Funkcja kontroli urządzeń rozpoznaje urządzenia przekierowywane za pomocą protokołów do pracy zdalnej Microsoft RDP, Citrix ICA, VMware PCoIP i HTML5/WebSockets w środowiskach wirtualizacji Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer i VMware Horizon hostowanych na chronionych komputerach z systemem Windows. Może też kontrolować operacje kopiowania danych między schowkiem systemu operacyjnego Windows gościa

© Acronis International GmbH, 2003-2024

działającego na urządzeniu VMware Workstation, VMware Player, Oracle VM VirtualBox lub Windows Virtual PC a schowkiem systemu operacyjnego hosta działającego na chronionym komputerze z systemem Windows.

Ten typ urządzeń jest obsługiwany tylko w systemie Windows.

Dostęp do przekierowywanych urządzeń można skonfigurować następująco:

- **Zamapowane dyski** — możesz zezwolić na pełny dostęp, zezwolić na dostęp tylko do odczytu lub odmówić dostępu w celu kontrolowania operacji kopiowania danych na dowolny dysk twardy, dysk wymienny lub napęd optyczny przekierowywany do sesji hostowanej bądź z takiego urządzenia w przypadku chronionego komputera.
- **Przychodzące dane schowka** — możesz zezwolić na dostęp lub odmówić dostępu w celu kontrolowania operacji kopiowania danych przez schowek do sesji hostowanej w przypadku chronionego komputera.

  Uwaga
  Po zmianie ustawienia dostępu w przypadku przychodzących danych schowka na **Odmów** trzeba uruchomić ponownie aplikacje i procesy uzyskujące dostęp do schowka w celu uwzględnienia nowo skonfigurowanych ustawień dostępu. Aby ustawienia dostępu były poprawnie egzekwowane, należy uruchomić ponownie chronione obciążenia.

- **Wychodzące dane schowka** — możesz zezwolić na dostęp lub odmówić dostępu w celu kontrolowania operacji kopiowania danych przez schowek z sesji hostowanej w przypadku chronionego komputera.

  Uwaga
  Po zmianie ustawienia dostępu w przypadku wychodzących danych schowka na **Odmów** trzeba uruchomić ponownie aplikacje i procesy uzyskujące dostęp do schowka w celu uwzględnienia nowo skonfigurowanych ustawień dostępu. Aby ustawienia dostępu były poprawnie egzekwowane, należy uruchomić ponownie chronione obciążenia.

- **Porty USB** — możesz zezwolić na dostęp lub odmówić dostępu w celu kontrolowania operacji kopiowania danych na urządzenia podłączane do dowolnego portu USB przekierowanego do sesji hostowanej bądź z tak podłączanych urządzeń w przypadku chronionego komputera.

Ustawienia kontroli urządzeń wpływają tak samo na wszystkich użytkowników. Jeśli na przykład skonfigurujesz odmowę dostępu do urządzeń wymiennych, uniemożliwisz każdemu użytkownikowi kopiowanie danych na te urządzenia oraz z tych urządzeń w przypadku chronionego komputera. Możliwe jest selektywne zezwalanie na dostęp do poszczególnych urządzeń USB przez wykluczanie ich z kontroli dostępu (zobacz Lista dozwolonych typów urządzeń i Lista dozwolonych urządzeń USB).

Jeśli dostęp do urządzenia jest kontrolowany zarówno na podstawie jego typu, jak i jego interfejsu, pierwszeństwo ma odmowa dostępu na poziomie interfejsu. Jeśli na przykład jest skonfigurowana odmowa dostępu do portów USB (interfejs urządzenia), to próby uzyskania dostępu do urządzeń mobilnych podłączonych do portu USB kończą się odmową bez względu na to, czy skonfigurowano

© Acronis International GmbH, 2003-2024

zezwolenie na dostęp czy odmowę dostępu do urządzeń mobilnych (typ urządzenia). Aby zezwolić na dostęp do takiego urządzenia, trzeba zezwolić zarówno na jego interfejs, jak i na jego typ.

Uwaga
Jeśli plan ochrony używany w systemie macOS obejmuje ustawienia dla typów urządzeń obsługiwanych tylko w systemie Windows, to ustawienia te będą ignorowane w systemie macOS.

Ważne
Jeśli do portu USB zostanie podłączone urządzenie wymienne, zaszyfrowane urządzenie wymienne, drukarka lub urządzenie Bluetooth, to zezwolenie na dostęp do tego urządzenia ma pierwszeństwo przed odmową dostępu skonfigurowaną na poziomie interfejsu USB. W przypadku zezwolenia na taki typ urządzeń dostęp do urządzenia jest dozwolony bez względu na to, czy skonfigurowano odmowę dostępu do portu USB.

Powiadomienia systemu operacyjnego i alerty usługi

Skonfiguruj funkcję kontroli urządzeń tak, aby wyświetlała użytkownikowi powiadomienia systemu operacyjnego, jeśli spróbuje on użyć urządzenia zablokowanego typu na chronionych komputerach. Jeśli w ustawieniach dostępu jest zaznaczone pole wyboru **Pokazuj powiadomienia systemu operacyjnego, jeśli użytkownicy spróbują użyć zablokowanego typu urządzenia lub portu**, agent wyświetli wyskakujące okienko z komunikatem w obszarze powiadomień chronionego komputera, jeśli wystąpi którekolwiek z poniższych zdarzeń:

- Odmowa w przypadku próby użycia urządzenia podłączonego do portu USB lub FireWire. To powiadomienie jest wyświetlane za każdym razem, gdy użytkownik podłączy urządzenie do portu USB lub FireWire, któremu ma zablokowany dostęp na poziomie interfejsu (na przykład w przypadku odmowy dostępu do portu USB) lub na poziomie typu (na przykład w przypadku odmowy dostępu do urządzeń wymiennych). Powiadomienie to zawiera informację, że użytkownik nie może uzyskiwać dostępu do wskazanego urządzenia/dysku.
- Odmowa w przypadku próby skopiowania obiektu danych (np. pliku) z określonego urządzenia. To powiadomienie jest wyświetlane w przypadku odmowy dostępu do odczytu w kontekście następujących urządzeń: stacje dyskietek, napędy optyczne, urządzenia wymienne, zaszyfrowane urządzenia wymienne, urządzenia mobilne, przekierowane dyski zamapowane i przekierowane dane przychodzące ze schowka. Powiadomienie to zawiera informację, że użytkownik nie może uzyskać określonego obiektu danych ze wskazanego urządzenia.

  Powiadomienie o odmowie odczytu jest też wyświetlane w przypadku odmowy dostępu do odczytu/zapisu w odniesieniu do połączeń Bluetooth, portu FireWire, portu USB i przekierowanego portu USB.
- Odmowa w przypadku próby skopiowania obiektu danych (np. pliku) na określone urządzenie. To powiadomienie jest wyświetlane w przypadku odmowy dostępu do zapisu na następujących urządzeniach: stacje dyskietek, napędy optyczne, urządzenia wymienne, zaszyfrowane urządzenia wymienne, urządzenia mobilne, lokalny schowek, rejestratory zrzutów ekranów, drukarki, przekierowane dyski zamapowane i przekierowane dane wychodzące ze schowka.

© Acronis International GmbH, 2003-2024

Powiadomienie to zawiera informację, że użytkownik nie może wysłać określonego obiektu danych na wskazane urządzenie.

Podejmowane przez użytkownika próby uzyskania dostępu do urządzeń zablokowanych typów na chronionych komputerach mogą wywoływać alerty, które są rejestrowane w konsoli Cyber Protect. Można włączyć alerty dla każdego typu urządzeń (z wyjątkiem rejestratorów zrzutów ekranu) lub portu z osobna, zaznaczając w ustawieniach dostępu pole wyboru **Pokaż alert**. Jeśli na przykład dostęp do urządzeń wymiennych jest ograniczony tylko do odczytu, a w przypadku urządzeń tego typu jest zaznaczone pole wyboru **Pokaż alert**, alert zostanie zarejestrowany za każdym razem, gdy użytkownik spróbuje na chronionym komputerze skopiować dane na urządzenie wymienne. Dodatkowe informacje można znaleźć w sekcji Alerty związane z kontrolą urządzeń.

Zobacz także instrukcję włączania lub wyłączania powiadomień systemu operacyjnego i alertów usługi.

Lista dozwolonych typów urządzeń

Na stronie **Lista dozwolonych typów urządzeń** można wybrać podklasy urządzeń, które mają być wykluczone z kontroli dostępu do urządzeń. W wyniku takich ustawień dostęp do tych urządzeń będzie dozwolony niezależnie od ustawień dostępu w module kontroli urządzeń.

Moduł kontroli urządzeń umożliwia zezwalanie na dostęp do urządzeń określonych podklas w ramach objętego odmową typu urządzeń. Ta opcja umożliwia zastosowanie odmowy wobec wszystkich urządzeń określonego typu, z wyjątkiem niektórych podklas urządzeń tego typu. Może to być przydatne na przykład wtedy, gdy trzeba odmówić dostępu do wszystkich portów USB, a jednocześnie zezwolić na korzystanie z klawiatury i myszy USB.

Podczas konfigurowania modułu kontroli urządzeń można określić podklasy urządzeń, które mają być wykluczone z kontroli dostępu do urządzeń. Gdy urządzenie należy do wykluczonej podklasy, dostęp do niego jest dozwolony, bez względu na to, czy danych typ urządzenia lub port są objęte odmową. Z kontroli dostępu do urządzeń można selektywnie wykluczać następujące podklasy urządzeń:

- **Urządzenia HID USB (mysz, klawiatura itd.)** — zaznaczenie tej opcji umożliwia dostęp do urządzeń interfejsu HID (myszy, klawiatury itp.) podłączonych do portów USB nawet wtedy, gdy jest aktywna odmowa dostępu do portów USB. Domyślnie ta pozycja jest zaznaczona, aby odmowa dostępu do portów USB nie skutkowała wyłączeniem klawiatury lub myszy.
  Opcja obsługiwana zarówno w systemie Windows, jak i macOS.
- **Karty sieciowe USB i FireWire** — zaznaczenie tej opcji umożliwia dostęp do kart sieciowych podłączonych do portów USB lub FireWire (IEEE 1394) nawet wtedy, gdy jest aktywna odmowa dostępu do portów USB i/lub FireWire.
  Opcja obsługiwana zarówno w systemie Windows, jak i macOS.
- **Skanery i aparaty fotograficzne USB** — zaznaczenie tej opcji umożliwia dostęp do skanerów i aparatów fotograficznych podłączonych do portów USB nawet wtedy, gdy jest aktywna odmowa dostępu do portów USB.
  Opcja obsługiwana tylko w systemie Windows.

© Acronis International GmbH, 2003-2024

- **Urządzenia audio USB** — zaznaczenie tej opcji umożliwia dostęp do urządzeń audio, takich jak zestawy słuchawkowe i mikrofony, podłączonych do portów USB nawet wtedy, gdy jest aktywna odmowa dostępu do portów USB.
  Opcja obsługiwana tylko w systemie Windows.
- **Kamery USB** — zaznaczenie tej opcji umożliwia dostęp do kamer internetowych podłączonych do portów USB nawet wtedy, gdy jest aktywna odmowa dostępu do portów USB.
  Opcja obsługiwana tylko w systemie Windows.
- **Urządzenia HID Bluetooth (mysz, klawiatura itd.)** — zaznaczenie tej opcji umożliwia dostęp do urządzeń interfejsu HID (myszy, klawiatury itp.) podłączonych przez Bluetooth nawet wtedy, gdy jest aktywna odmowa dostępu do Bluetooth.
  Opcja obsługiwana tylko w systemie Windows.
- **Kopiowanie/wklejanie przy użyciu schowka w ramach aplikacji** — zaznaczenie tej opcji umożliwia kopiowanie/wklejanie danych przez schowek w ramach danej aplikacji nawet wtedy, gdy jest aktywna odmowa dostępu do schowka.
  Opcja obsługiwana tylko w systemie Windows.

Uwaga
Ustawienia dotyczące nieobsługiwanych podklas urządzeń są ignorowane, jeśli zostały skonfigurowane w zastosowanym planie ochrony.

Dodając typy urządzeń do listy dozwolonych, warto uwzględnić następujące wskazówki:

- Za pomocą listy dozwolonych typów urządzeń można zezwolić tylko na całą podklasę urządzeń. Nie można zezwolić na określony model urządzenia, a aktywować odmowę w odniesieniu do pozostałych urządzeń z tej samej podklasy. Na przykład wykluczenie kamer USB z kontroli dostępu do urządzeń umożliwi korzystanie z dowolnej kamery USB, bez względu na jej model i dostawcę. Informacje na temat zezwalania na poszczególne urządzenia/modele można znaleźć w sekcji Lista dozwolonych urządzeń USB.
- Typy urządzeń można wybierać tylko w ramach zamkniętej listy podklas urządzeń. Jeśli chcesz zezwolić na urządzenie z innej podklasy, nie możesz tego zrobić przy użyciu listy dozwolonych typów urządzeń. Na przykład nie można dodać do listy dozwolonych takiej podklasy jak czytniki kart inteligentnych USB. Aby zezwolić na korzystanie z czytnika kart inteligentnych USB w przypadku odmowy dostępu do portów USB, postępuj zgodnie z instrukcjami zawartymi w sekcji Lista dozwolonych urządzeń USB.
- Lista dozwolonych typów urządzeń działa tylko w przypadku urządzeń korzystających ze standardowych sterowników systemu Windows. Moduł kontroli urządzeń może nie rozpoznać podklasy niektórych urządzeń USB z zastrzeżonymi sterownikami. W związku z tym nie można zezwolić na dostęp do takich urządzeń USB za pomocą listy dozwolonych typów urządzeń. W takim przypadku można zezwolić na dostęp na zasadzie „na urządzenie/model” (zobacz Lista dozwolonych urządzeń USB).

© Acronis International GmbH, 2003-2024

Lista dozwolonych urządzeń USB

Lista dozwolonych ma umożliwiać korzystanie z określonych urządzeń USB niezależnie od innych ustawień kontroli urządzeń. Można do niej dodać wybrane urządzenia lub modele urządzeń, aby wyłączyć kontrolę dostępu w ich przypadku. Jeśli na przykład dodasz do listy dozwolonych urządzenie mobilne o unikatowym identyfikatorze, zezwolisz na korzystanie z tego konkretnego urządzenia nawet wtedy, gdy jest aktywna odmowa dostępu do wszystkich innych urządzeń USB.

Na stronie **Lista dozwolonych typów urządzeń** można wskazać określone urządzenia USB lub modele urządzeń USB, które mają być wykluczone z kontroli dostępu do urządzeń. W wyniku takich ustawień dostęp do tych urządzeń będzie dozwolony niezależnie od ustawień dostępu w module kontroli urządzeń.

Urządzenia można definiować na liście dozwolonych na dwa sposoby:

- Model urządzenia — zbiorcze wskazanie wszystkich urządzeń danego modelu. Każdy model urządzenia jest identyfikowany przez identyfikator dostawcy (VID) i identyfikator produktu (PID), na przykład USB\VID_0FCE&PID_E19E.

  Taka kombinacja identyfikatorów VID i PID wskazuje nie konkretne urządzenie, tylko model urządzenia. Dodając model urządzenia do listy dozwolonych urządzeń, zezwalasz na dostęp do każdego urządzenia danego modelu. W ten sposób można zezwolić na używanie na przykład drukarek USB określonego modelu.
- Unikatowe urządzenie — wskazanie konkretnego urządzenia. Każde unikatowe urządzenie jest identyfikowany przez identyfikator dostawcy (VID), identyfikator produktu (PID) i numer seryjny, na przykład USB\VID_0FCE&PID_E19E\D55E7FCA.

  Nie wszystkie urządzenia USB mają przypisany numer seryjny. Urządzenie można dodać do listy dozwolonych jako unikatowe urządzenie tylko pod warunkiem, że podczas produkcji przypisano mu numer seryjny. Może to być na przykład dysk flash USB, który ma unikatowy numer seryjny.

Aby dodać urządzenie do listy dozwolonych urządzeń, należy najpierw dodać je do bazy danych urządzeń USB. Następnie można dodać urządzenia do listy dozwolonych, wybierając je z tej bazy danych.

Listą dozwolonych zarządza się na osobnej stronie konfiguracji o nazwie **Lista dozwolonych urządzeń USB**. Każda pozycja na liście reprezentuje urządzenie lub model urządzenia i zawiera następujące pola:

- **Opis** — system operacyjny przypisuje podłączanemu urządzeniu USB określony opis. Opis ten można zmodyfikować w bazie danych urządzeń USB (zobacz stronę zarządzania bazą danych urządzeń USB).
- **Typ urządzenia** — ma wartość Unikatowy, jeśli pozycja listy reprezentuje unikatowe urządzenie, lub wartość Model, jeśli reprezentuje model urządzenia.
- **Tylko do odczytu** — w przypadku zaznaczenia tej opcji dozwolone jest tylko odbieranie danych z urządzenia. Jeśli urządzenie nie obsługuje dostępu tylko do odczytu, to dostęp do urządzenia będzie zablokowany. Aby umożliwić pełny dostęp do urządzenia, wyczyść to pole wyboru.

© Acronis International GmbH, 2003-2024

- **Inicjuj ponownie** — w przypadku zaznaczenia tej opcji urządzenie symuluje rozłączenie / ponowne połączenie po zalogowaniu się nowego użytkownika. Niektóre urządzenia USB wymagają ponownego zainicjowania, aby mogły działać, dlatego zalecamy zaznaczenie tego pola wyboru w przypadku takich urządzeń (myszy, klawiatury itp.). Zalecamy również wyczyszczenie tego pola wyboru w przypadku urządzeń pamięci masowej (dysków flash USB, napędów optycznych, zewnętrznych dysków twardych itp.).
  Moduł kontroli urządzeń może nie być w stanie ponownie zainicjować niektórych urządzeń USB z zastrzeżonymi sterownikami. W przypadku braku dostępu do takiego urządzenia USB trzeba je odłączyć od portu USB, a następnie podłączyć ponownie.

  Uwaga
  Pole **Inicjuj ponownie** jest domyślnie ukryte. Aby ją wyświetlić w tabeli, kliknij ikonę koła zębatego w prawym górnym rogu tabeli i zaznacz pole wyboru **Inicjuj ponownie**.

  Uwaga
  Pola **Tylko do odczytu** i **Inicjuj ponownie** nie są obsługiwane w systemie macOS. Jeśli te pola są skonfigurowane w zastosowanym planie ochrony, zostaną zignorowane.

Urządzenia/modele możesz dodawać do listy dozwolonych i usuwać z niej w następujący sposób:

- Kliknij **Dodaj z bazy danych** nad listą i wybierz odpowiednie urządzenia spośród tych, które są zarejestrowane w bazie danych urządzeń USB. Wybrane urządzenie zostanie dodane do listy, gdzie można skonfigurować jego ustawienia i potwierdzić zmiany.
- Kliknij **Zezwól na to urządzenie USB** w alercie z informacją o odmowie dostępu do urządzenia USB (zobacz Alerty związane z kontrolą urządzeń). Spowoduje to dodanie urządzenia do listy dozwolonych i do bazy danych urządzeń USB.
- Kliknij ikonę Usuń dostępną na końcu pozycji listy. Spowoduje to usunięcie danego urządzenia/modelu z listy dozwolonych.

Baza danych urządzeń USB

Moduł kontroli urządzeń prowadzi bazę danych urządzeń USB, z której można dodawać urządzenia do listy wykluczeń (zobacz Lista dozwolonych urządzeń USB). Urządzenie USB można zarejestrować w bazie danych na dowolny z następujących sposobów:

- Dodaj urządzenie na stronie, która pojawia się podczas dodawania urządzenia do listy wykluczeń (zobacz Strona zarządzania bazą danych urządzeń USB).
- Dodaj urządzenie z karty Urządzenia USB na panelu Inwentaryzacja komputera w konsoli Cyber Protect (zobacz Lista urządzeń USB na komputerze).
- Zezwól na dostęp z alertu o odmowie dostępu do urządzenia USB (zobacz Alerty związane z kontrolą urządzeń).

Zobacz także instrukcję dodawania lub usuwania urządzeń USB w ramach bazy danych.

© Acronis International GmbH, 2003-2024

Strona zarządzania bazą danych urządzeń USB

Podczas konfigurowania listy dozwolonych urządzeń USB można dodać urządzenie z bazy danych. W przypadku wybrania takiej opcji zostanie wyświetlona strona zarządzania z listą urządzeń. Na tej stronie można wyświetlić listę wszystkich urządzeń zarejestrowanych w bazie danych i wybrać urządzenia, które mają zostać dodane do listy dozwolonych, a także wykonać następujące operacje:

Rejestrowanie urządzenia w bazie danych

1. Kliknij **Dodaj do bazy danych** u góry strony.
2. W wyświetlonym oknie dialogowym **Dodaj urządzenie USB** wybierz komputer, do którego jest podłączone dane urządzenie USB.
   Na liście komputerów są wyświetlane tylko komputery działające w trybie online.
   Lista urządzeń USB jest wyświetlana tylko w przypadku komputerów z zainstalowanym agentem do ochrony przed utratą danych.
   Urządzenia USB są wyświetlane w widoku drzewa. Pierwszy poziom drzewa reprezentuje model urządzenia. Drugi poziom reprezentuje konkretne urządzenie danego modelu.
   Niebieska ikona obok opisu urządzenia oznacza, że jest ono aktualnie podłączone do komputera. Jeśli urządzenie nie jest podłączone do komputera, ta ikona jest wyszarzona.
3. Zaznacz pole wyboru odpowiadające urządzeniu USB, które ma zostać zarejestrowane, i kliknij **Dodaj do bazy danych**.

Zmienianie opisu urządzenia

1. Na stronie **Baza danych urządzeń USB** kliknij wielokropek (...) na końcu pozycji listy reprezentującej urządzenie, a następnie kliknij **Edytuj**.
2. W wyświetlonym oknie dialogowym wprowadź zmiany w opisie.

Usuwanie urządzenia z bazy danych

1. Kliknij wielokropek (...) na końcu pozycji listy reprezentującej urządzenie.
2. Kliknij **Usuń** i potwierdź usunięcie.

Na tej stronie listy znajdują się następujące informacje o poszczególnych urządzeniach:

- **Opis** — łatwy do odczytania identyfikator urządzenia. Opis można zmieniać stosownie do potrzeb.
- **Typ urządzenia** — ma wartość Unikatowy, jeśli pozycja listy reprezentuje unikatowe urządzenie, lub wartość Model, jeśli reprezentuje model urządzenia. Unikatowe urządzenie musi mieć numer seryjny wraz z identyfikatorem dostawcy (VID) i identyfikatorem produktu (PID), natomiast model urządzenia jest identyfikowany przy użyciu kombinacji identyfikatorów VID i PID.
- **Identyfikator dostawcy**, **Identyfikator produktu**, **Numer seryjny** — te wartości razem tworzą identyfikator urządzenia w formacie USB\VID_<identyfikator dostawcy>&PID_<identyfikator produktu>\<numer seryjny>.
- **Konto** — wskazuje dzierżawcę, w którego obszarze znajduje się dane urządzenie. Jest to dzierżawca zawierający konto użytkownika użyte do rejestracji urządzenia w bazie danych.

© Acronis International GmbH, 2003-2024

Uwaga
Ta kolumna jest domyślnie ukryta. Aby ją wyświetlić w tabeli, kliknij ikonę koła zębatego w prawym górnym rogu tabeli i wybierz **Konto**.

Pierwsza kolumna z lewej strony służy do wybierania urządzeń, które mają zostać dodane do listy dozwolonych: Zaznacz pole wyboru każdego urządzenia, które chcesz dodać, a następnie kliknij **Dodaj do listy dozwolonych**. Aby zaznaczyć lub wyczyścić wszystkie pola wyboru, kliknij pole wyboru w nagłówku kolumny.

Listę urządzeń można przeszukiwać lub filtrować:

- Kliknij **Szukaj** u góry strony i wprowadź szukany ciąg znaków. Na liście zostaną wyświetlone urządzenia, których opis pasuje do wpisanego ciągu znaków.
- Kliknij **Filtruj**, a następnie skonfiguruj i zastosuj filtr w wyświetlonym oknie dialogowym. Lista jest ograniczona do urządzeń o typie, identyfikatorze dostawcy, identyfikatorze produktu i koncie wybranym podczas konfigurowania filtru. Aby anulować filtr i wyświetlić listę wszystkich urządzeń, kliknij **Resetuj do ustawień domyślnych**.

Eksportowanie listy urządzeń USB dostępnych w bazie danych

Istnieje możliwość wyeksportowania listy urządzeń USB dodanych do bazy danych.

1. Otwórz plan ochrony urządzenia do edycji.
2. Kliknij ikonę strzałki obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij wiersz **Lista dozwolonych urządzeń USB**.
3. Na stronie listy dozwolonych urządzeń USB kliknij **Dodaj z bazy danych**.
4. Na wyświetlonej stronie zarządzania bazą danych urządzeń USB kliknij **Eksportuj**. Zostanie otwarte standardowe okno dialogowe przeglądania.
5. Wybierz lokalizację, w której chcesz zapisać plik, w razie potrzeby wprowadź nową nazwę pliku, a następnie kliknij **Zapisz**.

Lista urządzeń USB zostanie wyeksportowana do pliku JSON.

Możesz edytować wynikowy plik JSON, aby dodać lub usunąć urządzenia, a także zbiorczo wprowadzić zmiany w opisach urządzeń.

Importowanie listy urządzeń USB do bazy danych

Zamiast dodawać urządzenia USB przy użyciu interfejsu użytkownika konsoli Cyber Protect, można zaimportować listę urządzeń USB. Lista jest plikiem w formacie JSON.

Uwaga
Takie plik JSON można zaimportować do bazy danych, która nie zawiera urządzeń opisanych w pliku. Aby zaimportować zmodyfikowany plik do bazy danych, z której został wyeksportowany, trzeba najpierw tę bazę wyczyścić, ponieważ nie można importować zduplikowanych wpisów. Jeśli wyeksportujesz listę urządzeń USB, zmodyfikujesz ją i spróbujesz zaimportować do tej samej bazy danych bez wyczyszczenia jej, operacja importu się nie powiedzie.

© Acronis International GmbH, 2003-2024

1. Otwórz plan ochrony urządzenia do edycji.
2. Kliknij ikonę strzałki obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij wiersz **Lista dozwolonych urządzeń USB**.
3. Na stronie listy dozwolonych urządzeń USB kliknij **Dodaj z bazy danych**.
4. Na wyświetlonej stronie zarządzania bazą danych urządzeń USB kliknij **Importuj**.
   Zostanie otwarte okno dialogowe Importuj urządzenia USB z pliku.
5. Przeciągnij plik do zaimportowania lub przejrzyj dysk, aby ten plik znaleźć.

Konsola Cyber Protect sprawdzi, czy lista zawiera duplikaty wpisów, które już istnieją w bazie danych, i je pominie. Urządzenia USB nieznalezione w bazie danych zostaną do niej dodane.

Lista urządzeń USB na komputerze

Panel Inwentaryzacja komputera w konsoli Cyber Protect zawiera kartę **Urządzenia USB**. Jeśli komputer działa w trybie online i jest na nim zainstalowany agent do ochrony przed utratą danych, na karcie **Urządzenia USB** będzie wyświetlana lista wszystkich urządzeń USB, które kiedykolwiek były podłączone do tego komputera.

Urządzenia USB są wyświetlane w widoku drzewa. Pierwszy poziom drzewa reprezentuje model urządzenia. Drugi poziom reprezentuje konkretne urządzenie danego modelu.

Lista ta zawiera następujące informacje o poszczególnych urządzeniach:

- **Opis** — system operacyjny przypisuje opis podłączanemu urządzeniu USB. Opis ten może służyć jako łatwy do odczytania identyfikator urządzenia.
  Niebieska ikona obok opisu urządzenia oznacza, że jest ono aktualnie podłączone do komputera. Jeśli urządzenie nie jest podłączone do komputera, ta ikona jest wyszarzona.
- **Identyfikator urządzenia** — identyfikator, który system operacyjny przypisał do urządzenia. Identyfikator ma następujący format: USB\VID_<identyfikator dostawcy>&PID_<identyfikator produktu>\<numer seryjny>, przy czym <numer seryjny> jest opcjonalny. Przykłady: USB\VID_0FCE&PID_ADDE\D55E7FCA (urządzenie z numerem seryjnym); USB\VID_0FCE&PID_ADDE (urządzenie bez numeru seryjnego).

Aby dodać urządzenia do bazy danych urządzeń USB, zaznacz pola wyboru tych urządzeń, a następnie kliknij przycisk **Dodaj do bazy danych**.

Wykluczanie procesów z kontroli dostępu

Dostęp do schowka systemu Windows, rejestratorów zrzutów ekranu, drukarek i urządzeń mobilnych jest kontrolowany za pomocą punktów zaczepienia (hook) umieszczanych w procesach. Jeśli punkty zaczepienia nie zostaną dodane do procesów, dostęp do urządzeń nie będzie kontrolowany.

© Acronis International GmbH, 2003-2024

Uwaga
Wykluczanie procesów z kontroli dostępu nie jest obsługiwane w systemie macOS. Jeśli lista wykluczonych procesów jest skonfigurowana w zastosowanym planie ochrony, zostanie zignorowana.

Na stronie **Wykluczenia** można określić listę procesów, w których nie zostaną umieszczone punkty zaczepienia. W przypadku takich procesów nie będzie stosowana kontrola dostępu do schowka (lokalnego ani przekierowanego), rejestratorów zrzutów ekranu, drukarek ani urządzeń mobilnych.

Na przykład zastosowano plan ochrony odmawiający dostępu do drukarek, a następnie uruchomiono aplikację Microsoft Word. Próba drukowania z tej aplikacji zostanie zablokowana. Jeśli jednak dodasz proces Microsoft Word do listy wykluczeń, to do tej aplikacji nie zostanie dodany punkt zaczepienia. Dzięki temu drukowanie z aplikacji Microsoft Word nie będzie blokowane, natomiast drukowanie z innych aplikacji nadal będzie blokowane.

Aby dodać procesy do listy wykluczeń

1. Otwórz plan ochrony urządzenia do edycji:
   Kliknij wielokropek (...) widoczny obok nazwy planu ochrony i wybierz **Edytuj**.

   Uwaga
   Aby można było uzyskać dostęp do ustawień kontroli nad urządzeniami, w planie musi być włączona funkcja Kontrola urządzeń.

2. Kliknij strzałkę obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij wiersz **Wykluczenia**.
3. Na stronie **Wykluczenia** w wierszu **Procesy i foldery** kliknij **+Dodaj**.
4. Dodaj procesy, które mają być wykluczone z kontroli dostępu.
   Na przykład `C:\Folder\podfolder\proces.exe`.
   Można użyć symboli wieloznacznych:
   - * zastępuje dowolną liczbę znaków.
   - ? zastępuje jeden znak.

   Na przykład:
   ```
   C:\Folder\*
   *\Folder\PodFolder?\*
   *\proces.exe
   ```
5. Kliknij znacznik wyboru, a następnie kliknij **Gotowe**.
6. W planie ochrony kliknij **Zapisz**.
7. Uruchom ponownie wykluczone procesy, aby punkty zaczepienia na pewno zostały prawidłowo usunięte.

Wykluczone procesy będą miały dostęp do schowka, rejestratorów zrzutów ekranu, drukarek i urządzeń mobilnych niezależnie od ustawień dostępu tych urządzeń.

© Acronis International GmbH, 2003-2024

Aby usunąć proces z listy wykluczeń

Otwórz plan ochrony urządzenia do edycji:

Kliknij wielokropek (...) widoczny obok nazwy planu ochrony i wybierz **Edytuj**.

Uwaga
Aby można było uzyskać dostęp do ustawień kontroli nad urządzeniami, w planie musi być włączona funkcja Kontrola urządzeń.

1. Kliknij strzałkę obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij wiersz **Wykluczenia**.
2. Na stronie **Wykluczenia** kliknij ikonę kosza obok procesu, który chcesz usunąć z listy wykluczeń.
3. Kliknij **Gotowe**.
4. W planie ochrony kliknij **Zapisz**.
5. Uruchom ponownie proces, aby punkt zaczepienia został prawidłowo umieszczony.

Ustawienia dostępu z planu ochrony zostaną zastosowane do procesów usuniętych z listy wykluczeń.

Aby edytować proces na liście wykluczeń

1. Otwórz plan ochrony urządzenia do edycji:
   Kliknij wielokropek (...) widoczny obok nazwy planu ochrony i wybierz **Edytuj**.

   Uwaga
   Aby można było uzyskać dostęp do ustawień kontroli nad urządzeniami, w planie musi być włączona funkcja Kontrola urządzeń.

2. Kliknij strzałkę obok przełącznika **Kontrola urządzeń**, aby rozwinąć ustawienia, a następnie kliknij wiersz **Wykluczenia**.
3. Na stronie **Wykluczenia** kliknij ikonę **Edytuj** obok procesu, który chcesz edytować.
4. Zastosuj zmiany i kliknij znacznik wyboru, aby potwierdzić.
5. Kliknij **Gotowe**.
6. W planie ochrony kliknij **Zapisz**.
7. Uruchom ponownie edytowane procesy, aby się upewnić, czy zmiany zostały poprawnie zastosowane.

Alerty związane z kontrolą urządzeń

Funkcja kontroli urządzeń prowadzi dziennik zdarzeń, śledząc podejmowane przez użytkownika próby uzyskania dostępu do kontrolowanych typów urządzeń, portów lub interfejsów. Niektóre zdarzenia mogą wywoływać alerty, które są rejestrowane w konsoli Cyber Protect. Na przykład, moduł kontroli urządzeń można skonfigurować tak, aby uniemożliwiał korzystanie z urządzeń

© Acronis International GmbH, 2003-2024

wymiennych, powodując zarejestrowanie alertu za każdym razem, gdy użytkownik spróbuje skopiować dane na takie urządzenie lub z takiego urządzenia.

Konfigurując moduł kontroli urządzeń, można włączyć alerty dla większości pozycji z listy Typ urządzeń (z wyjątkiem rejestratorów zrzutów ekranu) lub Porty. W przypadku włączenia alertów każda próba wykonania przez użytkownika niedozwolonej operacji spowoduje wygenerowanie alertu. Jeśli na przykład dostęp do urządzeń wymiennych jest ograniczony tylko do odczytu, a w przypadku urządzeń tego typu jest zaznaczona opcja **Pokaż alert**, alert zostanie wygenerowany za każdym razem, gdy użytkownik spróbuje na chronionym komputerze skopiować dane na urządzenie wymienne.

Aby wyświetlić alerty w konsoli Cyber Protect, przejdź do sekcji **Monitorowanie** > **Alerty**. W ramach każdego alertu związanego z kontrolą urządzeń konsola udostępnia następujące informacje o danym zdarzeniu:

- **Typ** — Ostrzeżenie.
- **Status** — wyświetlany jest status „Zablokowano dostęp do urządzeń peryferyjnych”.
- **Komunikat** — wyświetlany jest komunikat „Zablokowano dostęp do urządzenia «<typ urządzenia lub port>» na komputerze «<nazwa komputera>»”. Na przykład: Zablokowano dostęp do urządzenia „Wymienne” na komputerze „ksiegowosc-pc”.
- **Data i godzina** — data i godzina zdarzenia.
- **Urządzenie** — nazwa komputera, na którym wystąpiło zdarzenie.
- **Nazwa planu** — nazwa planu ochrony, który spowodował zdarzenie.
- **Źródło** — typ urządzenia lub port, z którym jest związane zdarzenie. Na przykład w przypadku odmowy dostępu, gdy użytkownik spróbuje skorzystać z urządzenia wymiennego, pole to zawiera napis „Urządzenie wymienne”.
- **Czynność** — operacja, która spowodowała zdarzenie. Na przykład w przypadku odmowy dostępu, gdy użytkownik spróbuje skopiować dane na urządzenie, pole to zawiera napis „Zapis”. Dodatkowe informacje można znaleźć w sekcji Wartości pola Czynność.
- **Nazwa** — nazwa obiektu docelowego zdarzenia, np. pliku, który użytkownik próbował skopiować, lub urządzenia, którego użytkownik próbował użyć. Nie jest wyświetlana, jeśli nie można zidentyfikować obiektu docelowego.
- **Informacje** — dodatkowe informacje o urządzeniu docelowym zdarzenia, np. identyfikator urządzenia w przypadku urządzenia USB. Nie są wyświetlane, jeśli nie ma żadnych dodatkowych informacji o urządzeniu docelowym.
- **Użytkownik** — nazwa użytkownika, który spowodował zdarzenie.
- **Proces** — w pełni kwalifikowana ścieżka do pliku wykonywalnego aplikacji, która spowodowała zdarzenie. W niektórych przypadkach zamiast ścieżki może zostać wyświetlona nazwa procesu. Dane te nie są wyświetlane, jeśli nie ma informacji o procesie.

Jeżeli alert dotyczy urządzenia USB (w tym urządzeń wymiennych lub zaszyfrowanych urządzeń wymiennych), to administrator może bezpośrednio z poziomu alertu dodać urządzenie do listy dozwolonych, co uniemożliwi modułowi kontroli urządzeń ograniczanie dostępu do tego urządzenia.

© Acronis International GmbH, 2003-2024

Kliknięcie **Zezwól na to urządzenie USB** spowoduje dodanie urządzenia do listy dozwolonych urządzeń USB w konfiguracji modułu kontroli urządzeń, a także do bazy danych urządzeń USB w celu użytkowania w przyszłości.

Zobacz także instrukcję wyświetlania alertów związanych z kontrolą urządzeń.

Wartości pola Czynność

Pole **Czynność** alertu może zawierać następujące wartości:

- **Odczyt** — uzyskanie danych z urządzenia lub portu.
- **Zapis** — wysłanie danych na urządzenie lub port.
- **Formatuj** — bezpośredni dostęp (formatowanie, sprawdzanie dysku itp.) do urządzenia. Jeśli kontekście portu chodzi o urządzenie podłączone do tego portu.
- **Wysuń** — usunięcie urządzenia z systemu lub wysunięcie nośnika z urządzenia. Jeśli kontekście portu chodzi o urządzenie podłączone do tego portu.
- **Drukuj** — wysłanie dokumentu do drukarki.
- **Kopiuj dźwięk** — skopiowanie/wklejenie danych audio za pośrednictwem lokalnego schowka.
- **Kopiuj plik** — skopiowanie/wklejenie pliku za pośrednictwem lokalnego schowka.
- **Kopiuj obraz** — skopiowanie/wklejenie obrazu za pośrednictwem lokalnego schowka.
- **Kopiuj tekst** — skopiowanie/wklejenie tekstu za pośrednictwem lokalnego schowka.
- **Kopiuj nierozpoznaną zawartość** — skopiowanie/wklejenie innych danych za pośrednictwem lokalnego schowka.
- **Kopiuj dane RTF (obraz)** — skopiowanie/wklejenie obrazu za pośrednictwem lokalnego schowka przy użyciu formatu RTF.
- **Kopiuj dane RTF (plik)** — skopiowanie/wklejenie pliku za pośrednictwem lokalnego schowka przy użyciu formatu RTF.
- **Kopiuj dane RTF (tekst, obraz)** — skopiowanie/wklejenie tekstu wraz z obrazem za pośrednictwem lokalnego schowka przy użyciu formatu RTF.
- **Kopiuj dane RTF (tekst, plik)** — skopiowanie/wklejenie tekstu wraz z plikiem za pośrednictwem lokalnego schowka przy użyciu formatu RTF.
- **Kopiuj dane RTF (obraz, plik)** — skopiowanie/wklejenie obrazu wraz z plikiem za pośrednictwem lokalnego schowka przy użyciu formatu RTF.
- **Kopiuj dane RTF (tekst, obraz, plik)** — skopiowanie/wklejenie tekstu wraz z obrazem i plikiem za pośrednictwem lokalnego schowka przy użyciu formatu RTF.
- **Usuń** — usunięcie danych z urządzenia (na przykład urządzenia wymiennego, urządzenia mobilnego itp.).
- **Dostęp do urządzenia** — dostęp do jakiegoś urządzenia lub portu (na przykład urządzenia Bluetooth, portu USB itp.).
- **Przychodzący dźwięk** — skopiowanie/wklejenie danych audio z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka.

© Acronis International GmbH, 2003-2024

- **Przychodzący plik** — skopiowanie/wklejenie pliku z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka.
- **Przychodzący obraz** — skopiowanie/wklejenie obrazu z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka.
- **Przychodzący tekst** — skopiowanie/wklejenie tekstu z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka.
- **Przychodząca nierozpoznana zawartość** — skopiowanie/wklejenie innych danych z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka.
- **Przychodzące dane RTF (obraz)** — skopiowanie/wklejenie obrazu z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Przychodzące dane RTF (plik)** — skopiowanie/wklejenie pliku z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Przychodzące dane RTF (tekst, obraz)** — skopiowanie/wklejenie tekstu wraz z obrazem z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Przychodzące dane RTF (tekst, plik)** — skopiowanie/wklejenie tekstu wraz z plikiem z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Przychodzące dane RTF (obraz, plik)** — skopiowanie/wklejenie obrazu wraz z plikiem z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Przychodzące dane RTF (tekst, obraz, plik)** — skopiowanie/wklejenie tekstu wraz z obrazem i plikiem z komputera klienckiego do hostowanej sesji za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Włóż** — podłączenie urządzenia USB lub urządzenia FireWire.
- **Wychodzący dźwięk** — skopiowanie/wklejenie danych audio z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka.
- **Wychodzący plik** — skopiowanie/wklejenie pliku z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka.
- **Wychodzący obraz** — skopiowanie/wklejenie obrazu z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka.
- **Wchodzący tekst** — skopiowanie/wklejenie tekstu z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka.
- **Wychodząca nierozpoznana zawartość** — skopiowanie/wklejenie innych danych z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka.
- **Wychodzące dane RTF (obraz)** — skopiowanie/wklejenie obrazu z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Wychodzące dane RTF (plik)** — skopiowanie/wklejenie pliku z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.

© Acronis International GmbH, 2003-2024

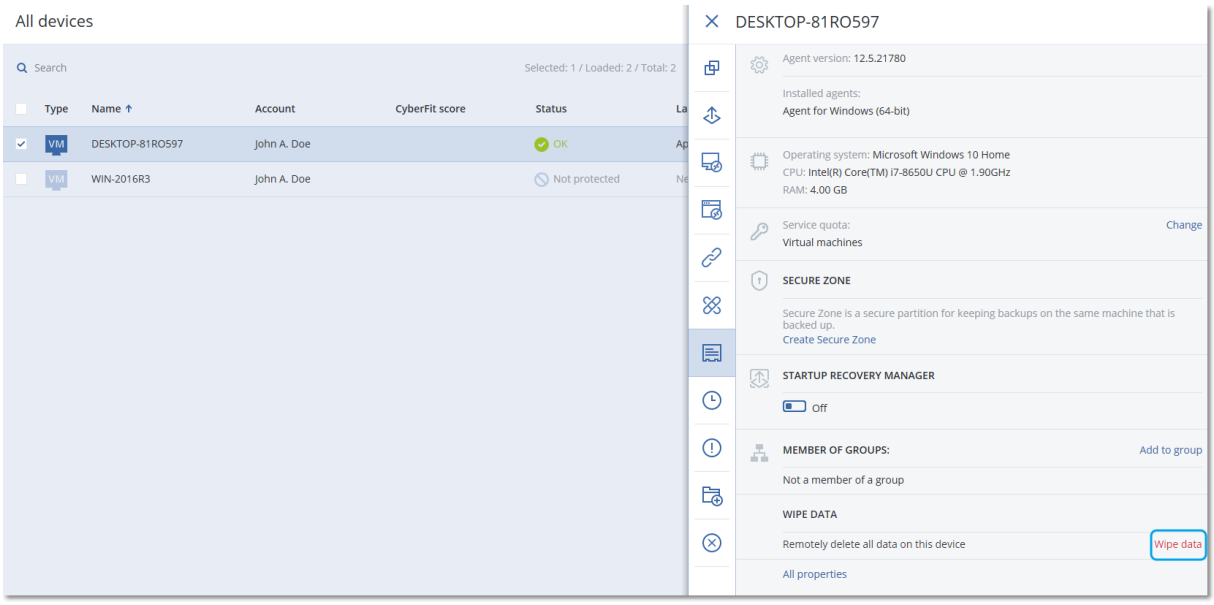
- **Wychodzące dane RTF (tekst, obraz)** — skopiowanie/wklejenie tekstu wraz z obrazem z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Wychodzące dane RTF (tekst, plik)** — skopiowanie/wklejenie tekstu wraz z plikiem z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Wychodzące dane RTF (obraz, plik)** — skopiowanie/wklejenie obrazu wraz z plikiem z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Wychodzące dane RTF (tekst, obraz, plik)** — skopiowanie/wklejenie tekstu wraz z obrazem i plikiem z hostowanej sesji na komputer kliencki za pośrednictwem przekierowanego schowka przy użyciu formatu RTF.
- **Zmień nazwę** — zmiana nazw plików na urządzeniu (na przykład na urządzeniach wymiennych, urządzeniach mobilnych i innych).

Wymazywanie danych z zarządzanego obciążenia

Uwaga
Zdalne wymazywanie jest dostępne w pakiecie Advanced Security.

Funkcja Wymazywanie zdalne umożliwia administratorowi usługi Cyber Protection i właścicielowi komputera usunięcie danych na komputerze zarządzanym, na przykład w przypadku jego zgubienia lub kradzieży. Zapobiegnie to nieuprawnionemu dostępowi do wrażliwych danych.

Zdalne wymazywanie jest dostępne tylko w przypadku komputerów z systemem Windows w wersji 10 lub nowszej. Aby otrzymać polecenie wymazania, komputer musi być włączony i podłączony do Internetu.



Aby wymazać dane z komputera

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputer, którego dane chcesz wymazać.

   Uwaga
   Dane można wymazywać tylko z pojedynczych komputerów.

3. Kliknij **Szczegóły**, a następnie kliknij **Wymaż dane**.
   Jeśli wybrany komputer jest w trybie offline, opcja **Wymaż dane** jest niedostępna.
4. Potwierdź wybór.
5. Podaj poświadczenia lokalnego administratora komputera i kliknij **Wymaż dane**.

   Uwaga
   Szczegóły procesu wymazywania i jego inicjatora można sprawdzić w sekcji **Monitorowanie** > **Działania**.

Obciążenia CyberApp

Obciążenia CyberApp są tworzone przez niezależnych dostawców oprogramowania (independent software vendor, ISV) i wyświetlane w konsoli Cyber Protect po włączeniu integracji CyberApp. Muszą zostać spełnione następujące warunki:

- W CyberApp musi być włączony punkt rozszerzeń **Obciążenia i czynności**.
- W CyberApp musi być zdefiniowany co najmniej jeden **Typ obciążenia**.
- Usługa łącznika hostowana przez dostawcę ISV musi zapewniać dodawanie i aktualizowanie obciążeń CyberApp na platformie Acronis.

Dodatkowe informacje na temat Portalu dostawców i tworzenia CyberApp można znaleźć w Podręczniku użytkownika Portalu dostawców.

Obciążenia zagregowane

Na obciążeniu fizycznym mogą być zainstalowane jednocześnie agent Cyber Protect i jeden lub kilka agentów CyberApp. W takim przypadku to samo obciążenie będzie miało więcej niż jedną reprezentację na ekranie **Wszystkie urządzenia** — zostanie wyświetlony osobny rekord dla obciążenia Acronis i każdego z obciążeń CyberApp. Jeśli w Portalu dostawców lub konsoli Cyber Protect zostanie włączone i skonfigurowane automatyczne scalanie obciążeń, system będzie porównywać adresy hostów i adresy MAC obciążeń Acronis oraz obciążeń CyberApp, po czym będzie łączyć wszystkie reprezentacje w jedno obciążenie zagregowane. Można też ręcznie scalać i rozłączać obciążenia w konsoli Cyber Protect.

Praca z obciążeniami CyberApp

Oprócz standardowych wbudowanych czynności dostępnych w konsoli Cyber Protect można wykonywać jeszcze czynności, które stają się dostępne po pojawieniu się obciążeń CyberApp w

© Acronis International GmbH, 2003-2024

konsoli: ręczne scalanie obciążeń w obciążenie zagregowane i wykonywanie czynności niestandardowych skonfigurowanych w CyberApp.

Scal

Wymagania wstępne

- W przypadku dzierżawcy są dostępne obciążenia z różnych źródeł.

Można ręcznie scalić obciążenie Acronis z jednym lub kilkoma obciążeniami CyberApp, w wyniku czego zostanie utworzone jedno obciążenie zagregowane.

Aby ręcznie scalić obciążenia w jedno obciążenie zagregowane

1. Na ekranie **Wszystkie urządzenia** kliknij obciążenia, które chcesz scalić.

   Uwaga
   Czynność scalania jest wyświetlana w przypadku wybrania obciążeń z różnych źródeł, takich jak obciążenie Acronis i obciążenie CyberApp.

2. Kliknij **Scal obciążenia**.

Wykonywanie czynności niestandardowych

Wymagania wstępne

- W przypadku dzierżawcy jest włączona integracja CyberApp, która ma zdefiniowane **Czynności dotyczące obciążenia**.

Czynności niestandardowe to czynności, które są skonfigurowane w środowisku CyberApp i stają się dostępne dla odpowiedniego obciążenia CyberApp po włączeniu integracji CyberApp dla dzierżawcy.

Aby wykonać czynności niestandardowe

1. Na ekranie **Wszystkie urządzenia** kliknij obciążenie.
2. Kliknij **Czynności dotyczące zintegrowanych aplikacji**.
3. Kliknij czynność.

Praca z obciążeniami zagregowanymi

Oprócz standardowych wbudowanych czynności dostępnych w konsoli Cyber Protect w odniesieniu do obciążeń zagregowanych można wykonywać jeszcze następujące operacje: wyświetlanie szczegółów, rozłączanie źródłowych obciążeń i wykonywanie niestandardowych czynności skonfigurowanych w CyberApps.

Wyświetl szczegóły

Wymagania wstępne

- W przypadku dzierżawcy jest dostępne co najmniej jedno obciążenie zagregowane.

© Acronis International GmbH, 2003-2024

Aby wyświetlić szczegóły obciążenia zagregowanego

1. Na ekranie **Wszystkie urządzenia** kliknij obciążenie zagregowane.
2. Kliknij opcję **Szczegóły**.

   Szczegóły obciążenia zagregowanego są wyświetlane z podziałem na karty. Na każdej karcie są widoczne szczegóły innej reprezentacji obciążenia.

Anuluj scalenie

Wymagania wstępne

- W przypadku dzierżawcy jest dostępne co najmniej jedno obciążenie zagregowane.

Po rozłączeniu obciążenia zagregowanego nie będzie ono już wyświetlane na liście urządzeń. Zamiast tego będą wyświetlane osobne pozycje dla każdego obciążenia źródłowego, które było scalone w ramach obciążenia zagregowanego.

Aby rozłączyć obciążenie zagregowane

1. Na ekranie **Wszystkie urządzenia** kliknij obciążenie zagregowane, które chcesz rozłączyć.
2. Kliknij **Anuluj scalenie obciążeń źródłowych**.
3. W oknie potwierdzenia kliknij **Anuluj scalenie**.

Wykonywanie czynności niestandardowych

Wymagania wstępne

- W przypadku dzierżawcy jest włączona co najmniej jedna integracja CyberApp, która ma zdefiniowane **Czynności dotyczące obciążenia**.

Czynności niestandardowe to czynności, które są skonfigurowane w CyberApps i stają się dostępne dla odpowiedniego obciążenia CyberApp po włączeniu integracji CyberApp dla dzierżawcy.

Aby wykonać czynności niestandardowe

1. Na ekranie **Wszystkie urządzenia** kliknij obciążenie.
2. Kliknij **Czynności dotyczące zintegrowanych aplikacji**.
3. W zależności od dostępnych czynności niestandardowych wykonaj jedną z poniższych czynności.
   - Jeśli obciążenie zagregowane ma jedno obciążenie CyberApp, kliknij czynność.
   - Jeśli obciążenie zagregowane ma więcej niż jedno obciążenie CyberApp, kliknij nazwę CyberApp, a następnie kliknij czynność.

Znajdź ostatniego zalogowanego użytkownika

Aby administratorzy mogli zarządzać urządzeniami, muszą zidentyfikować, który użytkownik jest i był zalogowany na urządzeniu. Informacje te są wyświetlane na pulpicie nawigacyjnym lub w sekcji szczegółów obciążenia.

© Acronis International GmbH, 2003-2024

Wyświetlanie informacji o ostatnim logowaniu w sekcji Plany zarządzania zdalnego można włączać lub wyłączać.

Na pulpicie nawigacyjnym:

1. Kliknij **Urządzenia**. Zostanie wyświetlone okno **Wszystkie urządzenia**.
2. W kolumnie **Ostatnie zalogowanie** jest wyświetlana nazwa użytkownika, który zalogował się jako ostatni w przypadku poszczególnych urządzeń.
3. W kolumnie **Godzina ostatniego zalogowania** jest wyświetlana godzina ostatniego zalogowania się użytkownika w przypadku poszczególnych urządzeń.

W sekcji Szczegóły urządzenia:

1. Kliknij **Urządzenia**. Zostanie wyświetlone okno **Wszystkie urządzenia**.
2. Kliknij urządzenie, w którego przypadku chcesz zweryfikować szczegóły.
3. Kliknij ikonę **Szczegóły**. Imię i nazwisko użytkownika oraz data i godzina ostatniego logowania w przypadku wybranego urządzenia są wyświetlane w sekcji **Ostatni zalogowani użytkownicy**.

Uwaga
W sekcji **Ostatni zalogowani użytkownicy** będzie wyświetlanych do 5 użytkowników, którzy się zalogowali na urządzeniu.

Aby wyświetlić lub ukryć kolumny Ostatnie zalogowanie i Godzina ostatniego zalogowania na pulpicie nawigacyjnym

1. Kliknij **Urządzenia**. Zostanie wyświetlone okno **Wszystkie urządzenia**.
2. Kliknij ikonę koła zębatego w prawym górnym rogu i w sekcji **Ogólne** wykonaj jedną z następujących czynności:
   - Włącz kolumny **Ostatnie zalogowanie** i **Godzina ostatniego zalogowania**, jeśli mają być wyświetlane na pulpicie nawigacyjnym.
   - Wyłącz kolumny **Ostatnie zalogowanie** i **Godzina ostatniego zalogowania**, jeśli mają być ukryte na pulpicie nawigacyjnym.

Wynik #CyberFit komputerów

Wynik #CyberFit stanowi mechanizm ocen zabezpieczeń oraz odpowiedniej punktacji, który pozwala badać poziom ogólnego bezpieczeństwa danego komputera. Identyfikuje on luki w zabezpieczeniach w środowisku IT i otwarte wektory ataków na urządzenia końcowe oraz przedstawia zalecane działania naprawcze w formie raportu. Ta funkcja jest dostępna we wszystkich wersjach programu Cyber Protect.

Funkcja Wynik #CyberFit jest obsługiwana w następujących systemach:

© Acronis International GmbH, 2003-2024

- Windows 7 (pierwsza wersja) i jego nowsze wersje
- Windows Server 2008 R2 i jego nowsze wersje

Sposób działania

Zainstalowany na komputerze agent ochrony przeprowadza ocenę zabezpieczeń i oblicza wynik #CyberFit komputera. Wynik #CyberFit komputera jest co jakiś czas automatycznie przeliczany.

Mechanizm obliczania wyniku #CyberFit

Wynik #CyberFit komputera jest obliczany według następujących wskaźników:

- Ochrona antywirusowa 0–275
- Ochrona kopii zapasowej 0–175
- Zapora 0–175
- Wirtualna sieć prywatna (VPN) 0–75
- Pełne szyfrowanie dysków 0–125
- Zabezpieczenia sieci 0–25

Maksymalny wynik #CyberFit komputera to 850.

Wskaźnik	Co podlega ocenie?	Zalecenia dla użytkowników	Punktacja
Ochrona antywirusowa	Agent sprawdza, czy na komputerze jest zainstalowane oprogramowanie antywirusowe.	Ustalenia: • Masz włączoną ochronę antywirusową (+275 punktów) • Nie masz ochrony antywirusowej. System jest narażony na niebezpieczeństwo (0 punktów) Zalecenia udostępniane przez funkcję Wynik #CyberFit: Na komputerze powinno być zainstalowane i włączone rozwiązanie antywirusowe, aby był on chroniony przed zagrożeniami bezpieczeństwa. Zapoznaj się z listą zalecanych rozwiązań antywirusowych w takich witrynach internetowych jak AV-Test czy AV-Comparatives.	275 — na komputerze jest zainstalowane oprogramowanie antywirusowe 0 — na komputerze nie ma zainstalowanego żadnego oprogramowania antywirusowego
Kopia zapasowa	Agent sprawdza, czy na komputerze jest zainstalowane	Ustalenia: • Masz rozwiązanie do tworzenia kopii zapasowych chroniące dane (+175	175 — na komputerze jest zainstalowane

© Acronis International GmbH, 2003-2024

	rozwiązanie do tworzenia kopii zapasowych.	punktów) • Nie znaleziono żadnego rozwiązania do tworzenia kopii zapasowych. Twoje dane są narażone na niebezpieczeństwo (0 punktów) Zalecenia udostępniane przez funkcję Wynik #CyberFit: Zaleca się regularne tworzenie kopii zapasowych danych, aby zapobiec ich utracie lub atakom przy użyciu oprogramowania ransomware. Oto kilka rozwiązań do tworzenia kopii zapasowych, których stosowanie warto rozważyć: • Acronis Cyber Protect / Cyber Backup / True Image • Kopia zapasowa systemu Windows Server (Windows Server 2008 R2 lub nowszy)	rozwiązanie do tworzenia kopii zapasowych 0 — na komputerze nie ma zainstalowanego żadnego rozwiązania do tworzenia kopii zapasowych
Zapora	Agent sprawdza, czy w środowisku jest dostępna i włączona zapora. Agent wykonuje następujące działania: 1. Sprawdza, czy w sekcjach Zapora systemu Windows i Ochrona sieci jest włączona zapora publiczna. 2. Sprawdza, czy w sekcjach Zapora systemu Windows i Ochrona sieci jest włączona zapora prywatna. 3. Jeśli publiczna i prywatna zapora systemu Windows jest wyłączona, sprawdza, czy jest	Ustalenia: • Masz włączoną zaporę na potrzeby sieci publicznych i prywatnych lub znaleziono rozwiązanie zapory innej firmy (+175 punktów) • Masz włączoną zaporę tylko na potrzeby sieci publicznych (+100 punktów) • Masz włączoną zaporę tylko na potrzeby sieci prywatnych (+75 punktów) • Nie masz włączonej żadnej zapory. Połączenie sieciowe nie jest bezpieczne (0 punktów) Zalecenia udostępniane przez funkcję Wynik #CyberFit: Zalecamy włączenie zapory dla sieci publicznej i prywatnej w celu wzmocnienia ochrony przed złośliwymi atakami na system. Poniżej znajdują się szczegółowe instrukcje konfiguracji zapory systemu Windows w zależności od potrzeb w zakresie bezpieczeństwa i architektury sieci:	100 — jest włączona publiczna zapora systemu Windows 75 —- jest włączona prywatna zapora systemu Windows 175 — jest włączona i publiczna, i prywatna zapora systemu Windows LUB jest włączone rozwiązanie zapory innej firmy 0 — nie włączono ani zapory systemu Windows, ani rozwiązania zapory innej firmy

© Acronis International GmbH, 2003-2024

	wyłączone rozwiązanie/agent zapory innej firmy.	Podręczniki dla użytkowników/pracowników: Jak skonfigurować zaporę Windows Defender na komputerze PC Jak skonfigurować zaporę systemu Windows na komputerze PC Podręczniki dla administratorów i inżynierów systemów: Jak wdrożyć zaporę Windows Defender przy użyciu zaawansowanych zabezpieczeń Jak utworzyć reguły zaawansowane w zaporze systemu Windows	
Wirtualna sieć prywatna (VPN)	Agent sprawdza, czy na komputerze jest zainstalowane rozwiązanie VPN oraz czy jest włączona i działa sieć VPN.	Ustalenia: • Masz rozwiązanie VPN i możesz bezpiecznie odbierać oraz wysyłać dane przez sieci publiczne i udostępnione (+75 punktów) • Nie znaleziono żadnego rozwiązania VPN. Połączenie z sieciami publicznymi i udostępnionymi nie jest bezpieczne (0 punktów) Zalecenia udostępniane przez funkcję Wynik #CyberFit: Zalecamy korzystanie z sieci VPN w celu uzyskiwania dostępu do firmowej sieci i poufnych danych. Sieć VPN jest niezwykle istotna dla zachowania bezpieczeństwa i prywatności komunikacji, zwłaszcza w przypadku korzystania z bezpłatnego dostępu do Internetu w kawiarni, w bibliotece, na lotnisku lub w innym miejscu. Oto kilka rozwiązań sieci VPN, których stosowanie warto rozważyć: • Firmowa sieć VPN Acronis • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN	75 — sieć VPN jest włączona i działa 0 — sieć VPN nie jest włączona

© Acronis International GmbH, 2003-2024

		• CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
Szyfrowanie dysku	Agent sprawdza, czy na komputerze jest włączone szyfrowanie dysków. Agent sprawdza, czy jest włączona funkcja Windows BitLocker.	Ustalenia: • Masz włączone pełne szyfrowanie dysków. Komputer jest chroniony przed manipulacjami fizycznymi (+125 punktów) • Zostały zaszyfrowane tylko niektóre dyski twarde. Komputer może być narażony na manipulacje fizyczne (+75 punktów) • Nie znaleziono szyfrowania dysku. Komputer jest narażony na manipulacje fizyczne (0 punktów) Zalecenia udostępniane przez funkcję Wynik #CyberFit: Zalecamy włączenie funkcji Windows BitLocker w celu wzmocnienia ochrony danych i plików. Podręcznik: Jak włączyć szyfrowanie urządzenia w systemie Windows	125 — są szyfrowane wszystkie dyski 75 — jest szyfrowany co najmniej jeden z używanych dysków, ale są też dyski nieszyfrowane 0 — nie jest szyfrowany żaden dysk
Zabezpieczenia sieci (wychodzący ruch NTLM do serwerów zdalnych)	Agent sprawdza, czy na komputerze ograniczono ruch NTLM wychodzący do serwerów zdalnych.	Ustalenia: • Odmowa wychodzącego ruchu NTLM do serwerów zdalnych. Twoje poświadczenia są chronione (+25 punktów) • Brak odmowy wychodzącego ruchu NTLM do serwerów zdalnych. Twoje poświadczenia są narażone na ujawnienie (0 punktów) Zalecenia udostępniane przez funkcję Wynik #CyberFit: Zalecamy odrzucanie wszelkiego ruchu NTLM wychodzącego do serwerów	25 — ustawienie wychodzącego ruchu NTLM ma wartość DenyAll 0 — ustawienie wychodzącego ruchu NTLM ma inną wartość

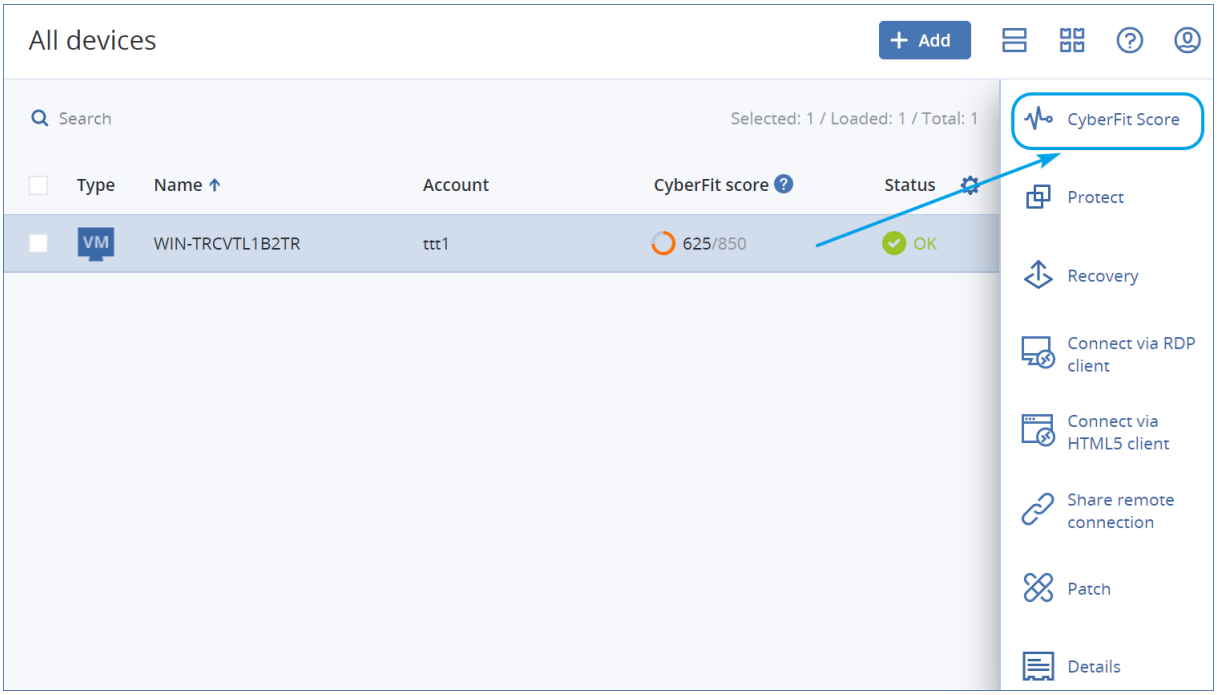
© Acronis International GmbH, 2003-2024

		zdalnych w celu wzmocnienia ochrony. Aby uzyskać informacje na temat zmieniania ustawień NTLM i dodawania wyjątków, kliknij poniższy link. Podręcznik: Ograniczanie wychodzącego ruchu NTLM do serwerów zdalnych	

Łączny wynik #CyberFit, obliczany przez zsumowanie punktów przyznanych za poszczególne wskaźniki, może odpowiadać jednej z poniższych ocen, która odzwierciedla poziom ochrony urządzenia końcowego:

- 0–579 — Słaby
- 580–669 — Przeciętny
- 670–739 — Dobry
- 740–799 — Bardzo dobry
- 800–850 — Znakomity

Wyniki #CyberFit komputerów można sprawdzać w konsoli Cyber Protect: przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**. Na liście urządzeń będzie dostępna kolumna **Wynik #CyberFit**. Można też uruchomić skanowanie w celu ustalenia wyniku #CyberFit komputera, aby sprawdzić poziom jego ogólnego bezpieczeństwa.



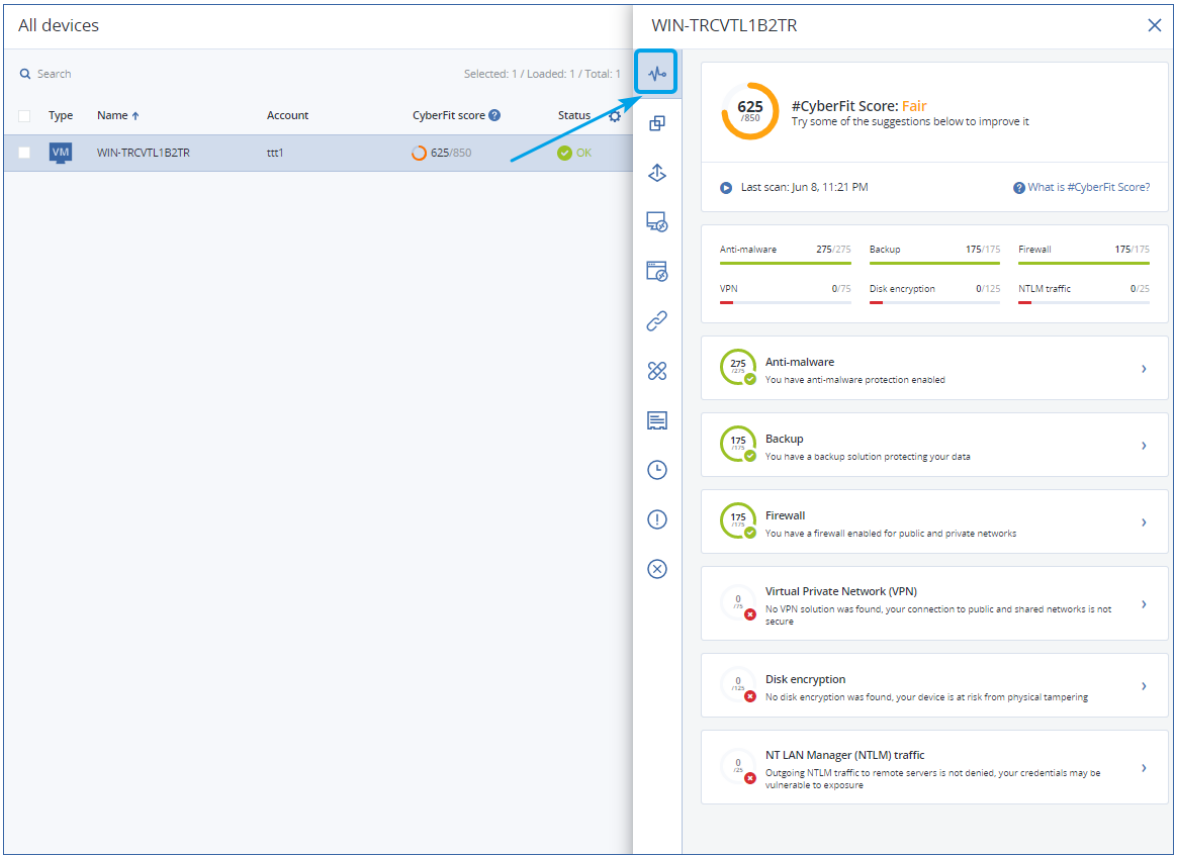
Informacje na temat wyników #CyberFit można też znaleźć na odpowiednich stronach widżetu i raportu.

© Acronis International GmbH, 2003-2024

Uruchamianie skanowania w celu ustalenia wyniku #CyberFit

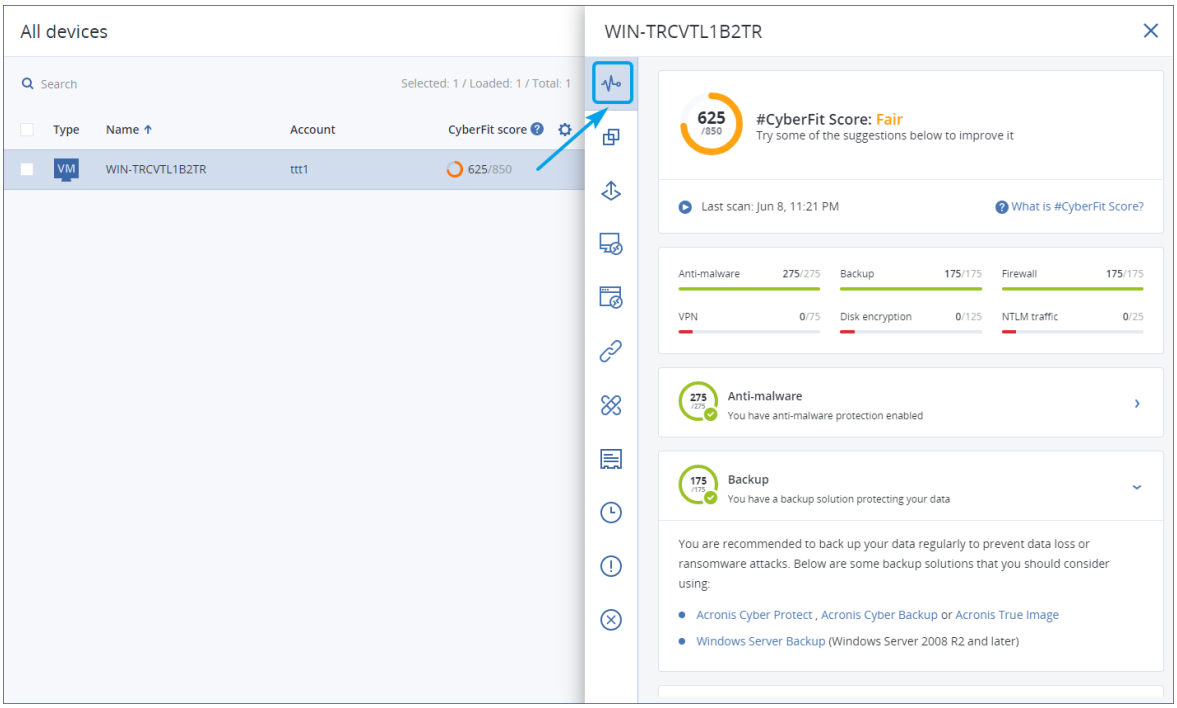
Aby uruchomić skanowanie w celu ustalenia wyniku #CyberFit

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Wybierz komputer i kliknij **Wynik #CyberFit**.
3. Jeśli komputer jeszcze nigdy nie był skanowany, kliknij **Uruchom pierwsze skanowanie**.
4. Po zakończeniu skanowania pojawi się łączny wynik #CyberFit komputera wraz z wynikami każdego z sześciu ocenianych wskaźników — Ochrona antywirusowa, Kopie zapasowe, Zapora, Wirtualna sieć prywatna (VPN), Szyfrowanie dysku oraz Ruch protokołu NT LAN Manager (NTLM).



5. Aby sprawdzić, jak można podwyższyć wynik w każdym ze wskaźników i które konfiguracje zabezpieczeń można poprawić, należy rozwinąć odpowiednią sekcję i zapoznać się z zaleceniami.

© Acronis International GmbH, 2003-2024



6. Po zastosowaniu się do zaleceń można ponownie obliczyć wynik #CyberFit komputera, klikając przycisk strzałki znajdujący się tuż pod łącznym wynikiem #CyberFit.

Skrypty cybernetyczne

Dzięki funkcji Skrypty cybernetyczne można za pomocą skryptów zautomatyzować rutynowe operacje na komputerach z systemem Windows i macOS w swoim środowisku, takie jak instalowanie oprogramowania, modyfikowanie konfiguracji, uruchamianie i zatrzymywanie usług oraz tworzenie kont. W ten sposób można skrócić czas poświęcany na takie operacje i zmniejszyć ryzyko popełnienia błędu w przypadku ich ręcznego wykonywania.

Skrypty cybernetyczne są dostępne dla administratorów i użytkowników na poziomie klienta, a także dla administratorów partnerów (usługodawców). Dodatkowe informacje o różnych poziomach administracji można znaleźć w sekcji "Obsługa wielu dzierżawców" (s. 322).

Skrypty, z których można korzystać, muszą zostać wcześniej zatwierdzone. Tylko administratorzy z rolą **Administrator środowiska cybernetycznego** mogą zatwierdzać i testować nowe skrypty. Więcej informacji na temat zmiany statusu skryptu można znaleźć w sekcji "Zmienianie statusu skryptu" (s. 410).

W zależności od roli użytkownika możesz wykonywać różne operacje dotyczące skryptów i planach skryptów. Więcej informacji na temat ról można znaleźć w sekcji "Role użytkowników a prawa do funkcji Skrypty cybernetyczne" (s. 400).

© Acronis International GmbH, 2003-2024

Wymagania wstępne

- Funkcja Skrypty cybernetyczne wymaga pakietu Advanced Management.
- Aby korzystać ze wszystkich możliwości funkcji Skrypty cybernetyczne, takich jak edycja skryptów, uruchamianie skryptów, tworzenie planów skryptów itd., należy włączyć dla swojego konta uwierzytelnianie dwuskładnikowe.

Ograniczenia

- Obsługiwane są następujące języki skryptów:
  - PowerShell
  - Bash
- Operacje wykonywane przy użyciu funkcji Skrypty cybernetyczne mogą być uruchamiane tylko na tych docelowych komputerach, na których jest zainstalowany agent ochrony.

Obsługiwane platformy

Skrypty cybernetyczne są dostępne w przypadku obciążeń z systemami Windows i macOS.

W poniższej tabeli zestawiono obsługiwane wersje.

System operacyjny	Wersja
Windows	Windows 7 SP1 i nowsze — wszystkie wersje
	Windows 8/8.1 — wszystkie wersje (x86, x64) z wyjątkiem systemu Windows RT
	Windows 10 — wersje Home, Pro, Education, Enterprise i IoT Enterprise
	Windows 11
	Windows Server 2008 R2 SP1 i nowsze — wersje Standard, Enterprise, Datacenter, Foundation i Web
	Windows Server 2012/2012 R2 — wszystkie wersje
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server (2008 R2, 2012, 2012 R2, 2016)

© Acronis International GmbH, 2003-2024

System operacyjny	Wersja
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

Role użytkowników a prawa do funkcji Skrypty cybernetyczne

Czynności dostępne w przypadku skryptów i planów skryptów zależą od statusu skryptu i roli użytkownika.

Administratorzy mogą zarządzać obiektami w ramach własnego dzierżawcy oraz jego dzierżawców podrzędnych. Nie widzą obiektów na wyższym poziomie administracji, jeśli taki poziom istnieje, ani nie mogą uzyskiwać do nich dostępu.

Administratorzy niższych poziomów mają dostęp tylko do odczytu do planów skryptów stosowanych do ich obciążeń roboczych przez administratora wyższego poziomu.

Poniższe role zapewniają prawa związane z funkcją Skrypty cybernetyczne:

- **Administrator firmy**
  Ta rola oznacza przyznanie pełnych praw administratora w przypadku wszystkich usług. Jeśli chodzi o funkcję Skrypty cybernetyczne, zapewnia ona takie same prawa jak rola Administrator środowiska cybernetycznego.
- **Administrator środowiska cybernetycznego**
  Ta rola oznacza przyznanie pełnych uprawnień, w tym do zatwierdzania skryptów, które mogą być używane w ramach dzierżawcy, oraz do uruchamiania skryptów ze statusem **Testowanie**.
- **Administrator**
  Ta rola oznacza przyznanie częściowych uprawnień, w tym możliwość uruchamiania zatwierdzonych skryptów, a także tworzenia i uruchamiania planów skryptów korzystających z zatwierdzonych skryptów.
- **Administrator w trybie tylko do odczytu**
  Ta rola oznacza przyznanie ograniczonych uprawnień, w tym możliwości wyświetlania skryptów i planów ochrony używanych w ramach dzierżawcy.
- **Użytkownik**
  Ta rola oznacza przyznanie częściowych uprawnień, w tym możliwość uruchamiania zatwierdzonych skryptów, a także tworzenia i uruchamiania planów skryptów korzystających z zatwierdzonych skryptów, ale tylko na komputerze użytkownika.

W poniższej tabeli zestawiono wszystkie dostępne czynności z uwzględnieniem statusu skryptu i roli użytkownika.

© Acronis International GmbH, 2003-2024

Rola	Obiekt	Status skryptu		
		Wersja robocza	**Testowanie**	**Zatwierdzono**
Administrator środowiska cybernetycznego **Administrator firmy**	Plan skryptów	Edytuj (usuń z planu roboczą wersję skryptu) Usuń Odwołaj Wyłącz Zatrzymaj	Utwórz Edytuj Zastosuj Włącz Uruchom Usuń Odwołaj Wyłącz Zatrzymaj	Utwórz Edytuj Zastosuj Włącz Uruchom Usuń Odwołaj Wyłącz Zatrzymaj
	Script	Utwórz Edytuj Zmień status Klonuj Usuń Anuluj uruchomienie	Utwórz Edytuj Zmień status Uruchom Klonuj Usuń Anuluj uruchomienie	Utwórz Edytuj Zmień status Uruchom Klonuj Usuń Anuluj uruchomienie
Administrator **Użytkownik** (w przypadku własnych maszyn)	Plan skryptów	Widok Odwołaj Wyłącz Zatrzymaj	Widok Anuluj przebieg	Utwórz Edytuj Zastosuj Włącz Uruchom Usuń Odwołaj Wyłącz Zatrzymaj
	Script	Utwórz Edytuj Klonuj	Widok Klonuj Anuluj	Uruchom Klonuj Anuluj

© Acronis International GmbH, 2003-2024

		Usuń Anuluj uruchomienie	uruchomienie	uruchomienie
Administrator w trybie tylko do odczytu	Plan skryptów	Widok	Widok	Widok
	Script	Widok	Widok	Widok

Skrypty

Skrypt to zestaw instrukcji, które są interpretowane w środowisku wykonawczym i wykonywane na komputerze docelowym. Skrypty stanowią wygodne rozwiązanie do automatyzacji powtarzających się lub złożonych zadań.

Za pomocą funkcji Skrypty cybernetyczne można uruchamiać predefiniowane skrypty lub tworzyć własne. Wszystkie skrypty dostępne dla Ciebie możesz wyświetlić w sekcji **Zarządzanie** > **Repozytorium skryptów**. Wstępnie zdefiniowane skrypty znajdują się w sekcji **Biblioteka**. Skrypty utworzone lub sklonowane do obszaru dzierżawcy, znajdują się w sekcji **Moje skrypty**.

Skryptu można użyć przez uwzględnienie go w planie skryptów lub wykonanie operacji **Szybkie uruchomienie skryptu**.

Uwaga
Można używać tylko zatwierdzonych skryptów utworzonych w ramach dzierżawcy lub sklonowanych do jego obszaru. Skrypt usunięty z repozytorium skryptów lub mający status **Wersja robocza** nie zostanie uruchomiony. Szczegółowe informacje o operacji wykonanej przy użyciu skryptu lub opcja jej anulowania są dostępne w sekcji **Monitorowanie** > **Działania**.

W poniższej tabeli udostępniono dodatkowe informacje na temat czynności, które można wykonać przy użyciu skryptu, w zależności od jego statusu.

Status	Możliwe czynności
Wersja robocza	Nowo utworzone skrypty oraz skrypty sklonowane do repozytorium mają status **Wersja robocza**. Skryptów tych nie możesz uruchamiać ani uwzględniać w planach skryptów.
Testowanie	Administratorzy z rolą **Administrator środowiska cybernetycznego** mogą uruchamiać te skrypty i uwzględniać je w planach skryptów.
Zatwierdzono	Możesz uruchamiać te skrypty i uwzględniać je w planach skryptów.

Tylko administratorzy z rolą **Administrator środowiska cybernetycznego** może zmienić status skryptu lub usunąć zatwierdzony skrypt. Dodatkowe informacje można znaleźć w sekcji "Zmienianie statusu skryptu" (s. 410).

© Acronis International GmbH, 2003-2024

Tworzenie skryptu

Możesz utworzyć skrypt, ręcznie pisząc kod.

Aby utworzyć skrypt

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Repozytorium skryptów**.
2. W obszarze **Moje skrypty** kliknij **Utwórz skrypt przy użyciu AI**.
3. W głównym okienku wpisz treść skryptu.

Ważne
Podczas tworzenia skryptu należy uwzględnić sprawdzanie kodu zakończenia dla każdej operacji. W przeciwnym razie nieudana operacja może zostać zignorowana i status aktywności skryptu w sekcji **Monitorowanie** > **Działania** może być niepoprawnie wyświetlany jako **Wykonane pomyślnie**.

4. Określ ustawienia skryptu.

Ustawienie	Opis
Nazwa skryptu	Nazwa skryptu. Pole jest wypełniane automatycznie, ale wartość można zmienić.
Opis	Opis skryptu. To ustawienie jest opcjonalne. [W przypadku skryptów generowanych przez AI] Po wygenerowaniu skryptu pole zostanie wypełnione automatycznie. Opis podany przez AI można edytować.
Język	Język skryptu. Dostępne wartości: • **PowerShell**. Jest to wartość domyślna. • **Bash** [W przypadku skryptów generowanych przez AI] To ustawienie jest konfigurowane przed wygenerowaniem skryptu.
System operacyjny	System operacyjny zainstalowany na maszynie docelowej, na której będzie uruchamiany skrypt. Dostępne wartości: • **Windows**. Jest to wartość domyślna. • **macOS** [W przypadku skryptów generowanych przez AI] To ustawienie jest konfigurowane przed wygenerowaniem skryptu.
Status	Status skryptu. • **Wersja robocza**. Jest to wartość domyślna. Nowo utworzone skrypty oraz skrypty sklonowane do repozytorium mają status **Wersja robocza**. Skryptów o statusie **Wersja robocza** nie możesz uruchamiać ani uwzględniać w planach skryptów. • **Testowanie**. Tylko administratorzy z rolą **Administrator środowiska cybernetycznego** mogą zmieniać status skryptu na **Testowanie**, uruchamiać skrypty o statusie **Testowanie** i uruchamiać plany skryptów przy użyciu takich

© Acronis International GmbH, 2003-2024

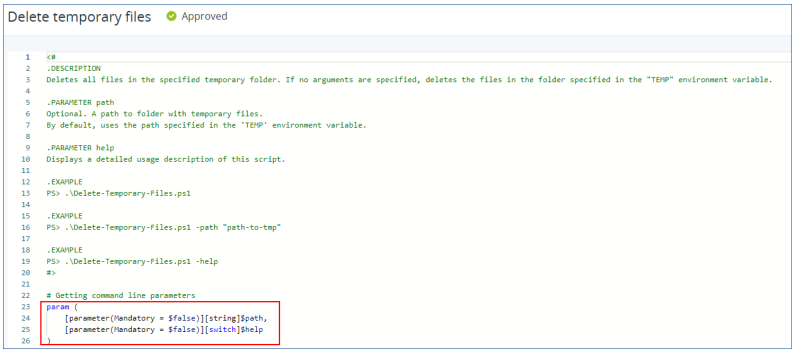
Ustawienie	Opis
	skryptów. • **Zatwierdzono**. Możesz uruchamiać skrypty o statusie **Zatwierdzono** i uwzględniać je w planach skryptowych. Tylko administratorzy z rolą **Administrator środowiska cybernetycznego** może zmienić status skryptu lub usunąć zatwierdzony skrypt. Dodatkowe informacje można znaleźć w sekcji "Zmienianie statusu skryptu" (s. 410).
Znaczniki	W znacznikach nie jest rozróżniana wielkość liter, a ich długość może wynosić maksymalnie 32 znaki. Nie można używać nawiasów okrągłych, nawiasów ostrokątnych, przecinków ani spacji. To ustawienie jest opcjonalne. [W przypadku skryptów wygenerowanych przez AI] Znacznik o statusie **Wygenerowane przez AI** zostanie dodany automatycznie podczas generowania skryptu. Możesz ręcznie go usunąć lub dodać więcej znaczników.

5. [Dotyczy tylko skryptów, które wymagają poświadczeń] Podaj poświadczenia.

   Można użyć jednego poświadczenia (np. tokenu) lub pary poświadczeń (np. nazwy użytkownika i hasła).
6. [Dotyczy tylko skryptów, które wymagają argumentów] Podaj argumenty i ich wartości w sposób następujący:
   a. Kliknij **Dodaj**.
   b. W polu **Dodaj argumenty** podaj argument.
   c. Kliknij **Dodaj**.
   d. W drugim wyświetlonym polu podaj wartość argumentu.

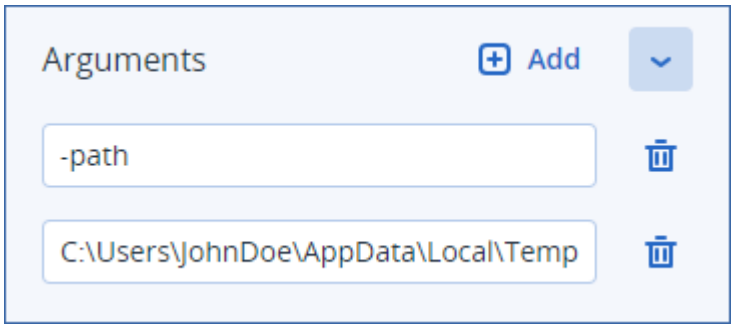
Uwaga

Możesz określić tylko te argumenty, które zostały zdefiniowane w treści skryptu.



Na przykład:

© Acronis International GmbH, 2003-2024



e. Powtórz powyższe kroki, jeśli chcesz dodać więcej niż jeden argument.

7. Kliknij **Zapisz**.

Skrypt zostanie zapisany w repozytorium ze statusem **Wersja robocza**.

Nie możesz używać skryptu, dopóki administrator z rolą **Administrator środowiska cybernetycznego** nie zmieni jego statusu na **Zatwierdzono**. Aby uzyskać więcej informacji, zobacz sekcję "Zmienianie statusu skryptu" (s. 410).

Aby użyć skryptu w ramach innego dzierżawcy, którym zarządzasz, musisz sklonować skrypt do tego dzierżawcy. Aby uzyskać więcej informacji, zobacz sekcję "Klonowanie skryptu" (s. 408).

Tworzenie skryptu przy użyciu AI

Uwaga
Ta funkcja wymaga pakietu Zarządzanie zaawansowane.

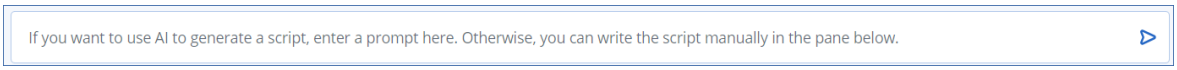
Dostępna jest możliwość użycia sztucznej inteligencji do przerabiania monitów na zaawansowane skrypty, co zapewnia oszczędność czasu i nakładów pracy. Funkcje te można wykorzystać następująco:

- Wprowadź prompt, aby spowodować, że mechanizm sztucznej inteligencji wygeneruje skrypt od podstaw.
- Wprowadź monit, aby spowodować, że mechanizm sztucznej inteligencji sprawdzi i uzupełni kod w treści skryptu. Możesz skorzystać z tej możliwości, gdy zmagasz się z bardziej złożonym kodem.

Funkcja ta wykorzystuje model GPT-4 OpenAI. Za jej pomocą można bezpłatnie utworzyć dla swojej organizacji do 100 skryptów w miesiącu kalendarzowym.

Aby utworzyć skrypt przy użyciu AI

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Repozytorium skryptów**.
2. W obszarze **Moje skrypty** kliknij **Utwórz skrypt przy użyciu AI**.
3. W wierszu polecenia wprowadź opis działania skryptu. Zadbaj, aby wprowadzony opis był jak najbardziej przejrzysty i szczegółowy.

   Na przykład:

© Acronis International GmbH, 2003-2024

```
I need a script that deletes Temporary files for all users (including user profiles +
Windows Temps) and disable Windows Update Service to allow the script to run
```

4. W prompcie przycisk strzałki.
5. W oknie potwierdzenia wybierz Język i System operacyjny, a następnie kliknij **Wygeneruj**.
   Skrypt wygenerowany przez AI jest wyświetlany w okienku głównym. Nazwa i opis skryptu są automatycznie generowane przez AI, tak aby pasowały do skryptu. Tag **Wygenerowane przez AI** jest automatycznie przypisywany do skryptu.
6. Przejrzyj skrypt wygenerowany przez AI i w razie potrzeby edytuj go ręcznie.
7. W razie potrzeby edytuj ustawienia skryptu.

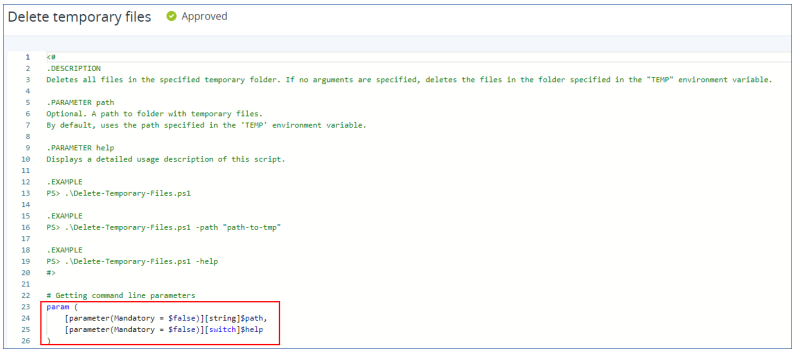
Ustawienie	Opis
Nazwa skryptu	Nazwa skryptu. Pole jest wypełniane automatycznie, ale wartość można zmienić.
Opis	Opis skryptu. To ustawienie jest opcjonalne. [W przypadku skryptów generowanych przez AI] Po wygenerowaniu skryptu pole zostanie wypełnione automatycznie. Opis podany przez AI można edytować.
Język	Język skryptu. Dostępne wartości: • **PowerShell**. Jest to wartość domyślna. • **Bash** [W przypadku skryptów generowanych przez AI] To ustawienie jest konfigurowane przed wygenerowaniem skryptu.
System operacyjny	System operacyjny zainstalowany na maszynie docelowej, na której będzie uruchamiany skrypt. Dostępne wartości: • **Windows**. Jest to wartość domyślna. • **macOS** [W przypadku skryptów generowanych przez AI] To ustawienie jest konfigurowane przed wygenerowaniem skryptu.
Status	Status skryptu. • **Wersja robocza**. Jest to wartość domyślna. Nowo utworzone skrypty oraz skrypty sklonowane do repozytorium mają status **Wersja robocza**. Skryptów o statusie **Wersja robocza** nie możesz uruchamiać ani uwzględniać w planach skryptów. • **Testowanie**. Tylko administratorzy z rolą **Administrator środowiska cybernetycznego** mogą zmieniać status skryptu na **Testowanie**, uruchamiać skrypty o statusie **Testowanie** i uruchamiać plany skryptów przy użyciu takich skryptów. • **Zatwierdzono**. Możesz uruchamiać skrypty o statusie **Zatwierdzono** i uwzględniać je w planach skryptowych. Tylko administratorzy z rolą **Administrator środowiska cybernetycznego** może zmienić status skryptu lub usunąć zatwierdzony skrypt. Dodatkowe informacje można znaleźć w sekcji "Zmienianie statusu skryptu" (s. 410).

© Acronis International GmbH, 2003-2024

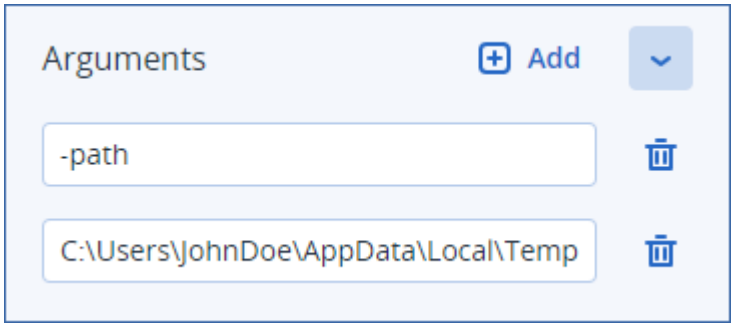
Ustawienie	Opis
Znaczniki	W znacznikach nie jest rozróżniana wielkość liter, a ich długość może wynosić maksymalnie 32 znaki. Nie można używać nawiasów okrągłych, nawiasów ostrokątnych, przecinków ani spacji. To ustawienie jest opcjonalne. [W przypadku skryptów wygenerowanych przez AI] Znacznik o statusie **Wygenerowane przez AI** zostanie dodany automatycznie podczas generowania skryptu. Możesz ręcznie go usunąć lub dodać więcej znaczników.

8. [Opcjonalnie] [Dotyczy tylko skryptów, które wymagają poświadczeń] Podaj poświadczenia. Można użyć jednego poświadczenia (np. tokenu) lub pary poświadczeń (np. nazwy użytkownika i hasła).
9. [Dotyczy tylko skryptów, które wymagają argumentów] Podaj argumenty i ich wartości w sposób następujący:
   a. Kliknij **Dodaj**.
   b. W polu **Dodaj argumenty** podaj argument.
   c. Kliknij **Dodaj**.
   d. W drugim wyświetlonym polu podaj wartość argumentu.

   Uwaga
   Możesz określić tylko te argumenty, które zostały zdefiniowane w treści skryptu.

   Na przykład:

   e. Powtórz powyższe kroki, jeśli chcesz dodać więcej niż jeden argument.
10. Kliknij **Zapisz**.

© Acronis International GmbH, 2003-2024

Skrypt zostanie zapisany w repozytorium ze statusem **Wersja robocza**.

Nie możesz używać skryptu, dopóki administrator z rolą **Administrator środowiska cybernetycznego** nie zmieni jego statusu na **Zatwierdzono**. Aby uzyskać więcej informacji, zobacz sekcję "Zmienianie statusu skryptu" (s. 410).

Aby użyć skryptu w ramach innego dzierżawcy, którym zarządzasz, musisz sklonować skrypt do tego dzierżawcy. Aby uzyskać więcej informacji, zobacz sekcję "Klonowanie skryptu" (s. 408).

Klonowanie skryptu

Sklonowanie skryptu jest konieczne w następujących przypadkach:

- Przed użyciem skryptu z obszaru **Biblioteka**. W takim przypadku należy najpierw sklonować skrypt do sekcji **Moje skrypty**.
- Gdy chcesz sklonować skrypty utworzone w ramach dzierżawcy nadrzędnego do obszarów dzierżawców podrzędnych lub jednostek.

Aby sklonować skrypt

1. W obszarze **Repozytorium skryptów** znajdź skrypt, który chcesz sklonować.
2. Wykonaj jedną z następujących czynności:
   - [W przypadku klonowania skryptu z sekcji **Moje skrypty**] Kliknij wielokropek (...) obok nazwy skryptu, a następnie kliknij **Klonuj**.
   - [W przypadku klonowania skryptu z obszaru **Biblioteka**] Kliknij **Klonuj** obok nazwy wybranego skryptu.
3. W wyskakującym oknie **Klonuj skrypt** na liście rozwijanej **Status** wybierz jeden z następujących statusów skryptu:
   - **Wersja robocza** (opcja domyślna) — ten status nie pozwala na wykonanie skryptu od razu.
   - **Testowanie** — ten status pozwala na wykonanie skryptu.
   - **Zatwierdzono** — ten status pozwala na wykonanie skryptu.
4. [W przypadku zarządzania więcej niż jednym dzierżawcą lub jednostką] Wybierz obszar, do którego chcesz sklonować skrypt.

   W oknie dialogowym **Klonuj skrypt** są widoczni tylko ci dzierżawcy, którymi możesz zarządzać i w których przypadku zastosowano pakiet Advanced Management.

W wyniku tych działań skrypt zostanie sklonowany do sekcji **Moje skrypty** wybranego dzierżawcy lub jednostki. W przypadku zarządzania tylko jednym dzierżawcą, w ramach którego nie ma żadnych jednostek, skrypt zostanie automatycznie skopiowany do sekcji **Moje skrypty**.

Ważne
Poświadczenia używane przez skrypt nie są kopiowane podczas klonowania skryptu do obszaru nieoryginalnego dzierżawcy.

© Acronis International GmbH, 2003-2024

Edytowanie lub usuwanie skryptu

Uwaga
W zależności od roli użytkownika możesz wykonywać różne operacje dotyczące skryptów i planach skryptów. Więcej informacji na temat ról można znaleźć w sekcji "Role użytkowników a prawa do funkcji Skrypty cybernetyczne" (s. 400).

Aby edytować skrypt

1. W obszarze **Repozytorium skryptów** przejdź do sekcji **Moje skrypty** i znajdź skrypt, który chcesz edytować.
2. Kliknij wielokropek (...) obok nazwy skryptu, a następnie kliknij **Edytuj**.
3. Edytuj skrypt i kliknij **Zapisz**.
4. [W przypadku edycji skryptu używanego w planie skryptów] Potwierdź wybór, klikając **Zapisz skrypt**.

   Uwaga
   Przy następnym uruchomieniu planu skryptów zostanie użyta najnowsza wersja skryptu.

Wersje skryptu

W przypadku edycji któregokolwiek z poniższych atrybutów skryptu jest tworzona nowa wersja skryptu:

- treść skryptu
- nazwa skryptu
- opis
- język skryptu
- poświadczenia
- argumenty

W przypadku zmiany innych atrybutów zmiany edycyjne zostaną dodane do bieżącej wersji skryptu. Więcej informacji o wersjach i ich porównywaniu można znaleźć w sekcji "Porównywanie wersji skryptu" (s. 411).

Uwaga
Status skryptu jest aktualizowany tylko wtedy, gdy zostanie zmieniona wartość w polu **Status**. Statusy skryptów mogą zmieniać tylko administratorzy z rolą Administrator środowiska cybernetycznego.

Aby usunąć skrypt

© Acronis International GmbH, 2003-2024

1. W obszarze **Repozytorium skryptów** przejdź do sekcji **Moje skrypty** i znajdź skrypt, który chcesz usunąć.
2. Kliknij wielokropek (...) obok nazwy skryptu, a następnie kliknij **Usuń**.
3. Kliknij **Usuń**.
4. [W przypadku usuwania skryptu używanego przez plan skryptów] Potwierdź wybór, klikając **Zapisz skrypt**.

Uwaga
Wykonywanie planów skryptów, w których był używany usunięty skrypt, będzie się kończyć niepowodzeniem.

Zmienianie statusu skryptu

Utworzonego nowego skryptu w stanie **Wersja robocza** nie można używać, dopóki jego status nie zostanie zmieniony na **Zatwierdzono**. W zależności od zastosowania skrypt może przez jakiś czas mieć status **Testowanie**, zanim zostanie zatwierdzony.

Uwaga
W zależności od roli użytkownika możesz wykonywać różne operacje dotyczące skryptów i planach skryptów. Więcej informacji na temat ról można znaleźć w sekcji "Role użytkowników a prawa do funkcji Skrypty cybernetyczne" (s. 400).

Wymagania wstępne

- Użytkownik jest administratorem z przypisaną rolą **Administrator środowiska cybernetycznego**.
- Dostępny jest skrypt ze zdefiniowanym odpowiednim stanem.

Aby zmienić status skryptu

1. W obszarze **Repozytorium skryptów** przejdź do sekcji **Moje skrypty**.
2. Kliknij wielokropek (...) obok nazwy skryptu, a następnie kliknij **Edytuj**.
3. Z listy rozwijanej **Status** wybierz status.
4. Kliknij **Zapisz**.
5. [W przypadku zmiany statusu zatwierdzonego skryptu] Aby potwierdzić zmianę, kliknij **Zapisz skrypt**.

Uwaga
Jeśli status skryptu został obniżony do poziomu **Wersja robocza**, korzystające z niego plany skryptów nie zostaną uruchomione.

Skrypty ze statusem **Testowanie** i plany skryptów z takimi skryptami mogą uruchamiać tylko administratorzy z rolą **Administrator środowiska cybernetycznego**.

© Acronis International GmbH, 2003-2024

Porównywanie wersji skryptu

Istnieje możliwość porównania dwóch wersji skryptu i powrotu do starszej wersji. Można też sprawdzić, kto i kiedy utworzył daną wersję.

Aby porównać wersje skryptu

1. W obszarze **Repozytorium skryptów** przejdź do sekcji **Moje skrypty** i znajdź skrypt, którego wersje chcesz porównać.
2. Kliknij wielokropek (...) obok nazwy skryptu, a następnie kliknij **Historia wersji**.
3. Wybierz dwie wersje, które chcesz porównać, i kliknij **Porównaj wersje**.
   Zostaną wyróżnione wszelkie zmiany w treści skryptu, jego argumentach i poświadczeniach.

Aby powrócić do starszej wersji

1. W oknie **Porównaj wersje skryptu** kliknij **Przywróć tę wersję**.
2. W wyskakującym okienku **Przywróć poprzednią wersję** wybierz status skryptu z listy rozwijanej **Status**.

Wybrana wersja zostanie przywrócona i zapisana w historii wersji jako najnowsza.

W celu przywrócenia skryptu możesz też wybrać wersję w oknie **Historia wersji**, a następnie kliknąć przycisk **Przywróć**.

Ważne
Możesz wykonywać tylko skrypty o statusie **Testowanie** lub **Zatwierdzone**. Aby uzyskać więcej informacji, zobacz sekcję "Zmienianie statusu skryptu" (s. 410).

Pobieranie danych wyjściowych operacji wykonanej przy użyciu skryptu

Dane wyjściowe operacji wykonanej przy użyciu skryptu można pobrać jako plik .zip. Zawiera on dwa pliki tekstowe: `stdout` i `stderr`. W pliku `stdout` znajdują się wyniki pomyślnie zakończonej operacji wykonanej przy użyciu skryptu. Plik `stderr` zawiera informacje o błędach, które wystąpiły podczas wykonywania skryptu.

Aby pobrać plik z danymi wyjściowymi

1. W konsoli Cyber Protect przejdź do sekcji **Monitorowanie** > **Działania**.
2. Kliknij działanie skryptów cybernetycznych, którego dane wyjściowe chcesz pobrać.
3. Na ekranie **Szczegóły działania** kliknij **Pobierz dane wyjściowe**.

Repozytorium skryptów

Repozytorium skryptów można znaleźć na karcie **Zarządzanie**. W repozytorium można wyszukiwać skrypty na podstawie ich nazw i opisów. Można też używać filtrów lub sortować skrypty według nazwy bądź statusu.

© Acronis International GmbH, 2003-2024

Aby zarządzać skryptem, kliknij wielokropek (...) obok jego nazwy, a następnie wybierz odpowiednią czynność. Można też kliknąć skrypt i skorzystać z przycisków dostępnych na otwartym ekranie.

Repozytorium skryptów zawiera następujące sekcje:

- **Moje skrypty**

  W tym miejscu znajdują się skrypty, których można bezpośrednio użyć we własnym środowisku. Są to skrypty, które zostały utworzone od podstaw oraz sklonowane w to miejsce.

  W tej sekcji można filtrować skrypty według następujących kryteriów:

  - Znaczniki
  - Status
  - Język
  - System operacyjny
  - Właściciel skryptu

- **Biblioteka**

  Biblioteka zawiera predefiniowane skrypty, których można używać we własnym środowisku po sklonowaniu ich do sekcji **Moje skrypty**. Skrypty te można tylko sprawdzać i klonować.

  W tej sekcji można filtrować skrypty według następujących kryteriów:

  - Znaczniki
  - Język
  - System operacyjny

  Aby uzyskać więcej informacji, zobacz artykuł 70595: Vendor-Approved Scripts (Skrypty zatwierdzone przez dostawcę).

Plany skryptów

Plan skryptów umożliwia uruchomienie skryptu w odniesieniu do wielu obciążeń, zaplanowanie uruchomienia skryptu oraz skonfigurowanie dodatkowych ustawień.

Utworzone plany skryptów i plany zastosowane do obciążeń można znaleźć w sekcji **Zarządzanie** > **Plany skryptów**. W tym miejscu można sprawdzić lokalizację wykonywania planu, jego właściciela lub status.

Na pasku, który można klikać, są wyświetlane następujące, oznaczone kolorami statusy planów skryptów:

- Uruchomiono (niebieski)
- Sprawdzanie kompatybilności (ciemnoszary)
- Wyłączono (jasnoszary)
- OK (zielony)
- Alert krytyczny (czerwony)

© Acronis International GmbH, 2003-2024

- Błąd (pomarańczowy)
- Ostrzeżenie (żółty)

  Klikając pasek, można sprawdzić, jaki status ma dany plan i na ilu obciążeniach. Można też kliknąć każdy status.

  Na karcie **Plany skryptów** można zarządzać planami, wykonując następujące czynności:

  - Uruchom
  - Zatrzymaj
  - Edytuj
  - Zmień nazwę
  - Wyłącz
  - Włącz
  - Klonuj
  - Eksportuj. Konfiguracja planu zostanie wyeksportowana na komputer lokalny w formacie JSON.
  - Usuń

  Widoczność planu skryptów i dostępne dzięki niemu działania zależą od właściciela planu i Twojej roli użytkownika. Na przykład administratorzy firm widzą tylko plany skryptów należące do partnerów, które są stosowane do ich obciążeń, i nie mogą wykonywać żadnych działań przy użyciu tych planów.

  Więcej informacji o tym, kto może tworzyć plany skryptów i nimi zarządzać, można znaleźć w sekcji "Role użytkowników a prawa do funkcji Skrypty cybernetyczne" (s. 400).

  Aby zarządzać planem skryptów

  1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany skryptów**.
  2. Znajdź plan, którym chcesz zarządzać, a następnie kliknij widoczny obok niego wielokropek (...).
  3. Wybierz odpowiednią czynność i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Tworzenie planu skryptów

Plan skryptów można utworzyć następująco:

- Na karcie **Urządzenia**
  Wybierz obciążenia, a następnie utwórz dla nich plan skryptów.
- Na karcie **Zarządzanie** > **Plany skryptów**
  Utwórz plan skryptów, a następnie wybierz obciążenia, do których ma on zostać zastosowany.

Aby utworzyć plan skryptów na karcie Urządzenia

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Wybierz obciążenia lub grupy urządzeń, do których chcesz zastosować plan skryptów, a następnie kliknij odpowiednio **Chroń** lub **Chroń grupę**.
3. [W przypadku już zastosowanych planów] Kliknij **Dodaj plan**.
4. Kliknij **Utwórz plan** > **Plan skryptów**.
   Zostanie otwarty szablon planu skryptów.
5. [Opcjonalnie] Aby zmienić nazwę planu skryptów, kliknij ikonę ołówka.
6. Kliknij **Wybierz skrypt**, wybierz skrypt, którego chcesz użyć, a następnie kliknij **Gotowe**.

   Uwaga
   Możesz używać tylko zatwierdzonych skryptów z sekcji **Repozytorium skryptów** > **Moje skrypty**. Skryptów ze statusem **Testowanie** może używać tylko administrator z rolą **Administrator środowiska cybernetycznego**. Dodatkowe informacje na temat ról można znaleźć w sekcji "Role użytkowników a prawa do funkcji Skrypty cybernetyczne" (s. 400).

7. Skonfiguruj harmonogram i warunki rozpoczęcia planu skryptów.
8. Wybierz konto, na którym skrypt będzie uruchamiany na docelowym obciążeniu. Dostępne są następujące opcje:
   - Konto systemowe (w systemie macOS jest to konto użytkownika root)
   - Aktualnie zalogowane konto
9. Określ, jak długo skrypt ma być wykonywany na docelowym obciążeniu.
   Jeśli skrypt nie zakończy działania w określonym czasie, operacja skryptów cybernetycznych zakończy się niepowodzeniem.
   Minimalna wartość, którą można określić, to 1 minuta, a maksymalna — 1440 minut.
10. [Tylko w przypadku skryptów PowerShell] Skonfiguruj zasady wykonywania programu PowerShell.
    Dodatkowe informacje na temat tych zasad można znaleźć w dokumentacji firmy Microsoft.
11. Kliknij **Utwórz**.

Aby utworzyć plan skryptów na karcie Plany skryptów

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany skryptów**.
2. Kliknij **Utwórz plan**.
   Zostanie otwarty szablon planu skryptów.
3. [Opcjonalnie] Aby wybrać obciążenia lub grupy urządzeń, do których chcesz zastosować nowy plan, kliknij **Dodaj obciążenia**.
   a. Kliknij **Komputery z agentami**, aby rozwinąć listę, a następnie wybierz odpowiednie obciążenia lub grupy urządzeń.
   b. Kliknij **Dodaj**.

   Dodatkowe informacje o tym, jak utworzyć grupy urządzeń na poziomie partnera, można znaleźć w sekcji "Karta Urządzenia" (s. 317).

© Acronis International GmbH, 2003-2024

Uwaga
Obciążenia lub grupy urządzeń można też wybrać po utworzeniu planu.

4. [Opcjonalnie] Aby zmienić nazwę planu skryptów, kliknij ikonę ołówka.
5. Kliknij **Wybierz skrypt**, wybierz skrypt, którego chcesz użyć, a następnie kliknij **Gotowe**.

Uwaga
Możesz używać tylko zatwierdzonych skryptów z sekcji **Repozytorium skryptów** > **Moje skrypty**. Skryptów ze statusem **Testowanie** może używać tylko administrator z rolą **Administrator środowiska cybernetycznego**. Dodatkowe informacje na temat ról można znaleźć w sekcji "Role użytkowników a prawa do funkcji Skrypty cybernetyczne" (s. 400).

6. Skonfiguruj harmonogram i warunki rozpoczęcia planu skryptów.
7. Wybierz konto, na którym skrypt będzie uruchamiany na docelowym obciążeniu. Dostępne są następujące opcje:
   - Konto systemowe (w systemie macOS jest to konto użytkownika root)
   - Aktualnie zalogowane konto
8. Określ, jak długo skrypt ma być wykonywany na docelowym obciążeniu.
   Jeśli skrypt nie zakończy działania w określonym czasie, operacja skryptów cybernetycznych zakończy się niepowodzeniem.
   Minimalna wartość, którą można określić, to 1 minuta, a maksymalna — 1440 minut.
9. [Tylko w przypadku skryptów PowerShell] Skonfiguruj zasady wykonywania programu PowerShell.
   Dodatkowe informacje na temat tych zasad można znaleźć w dokumentacji firmy Microsoft.
10. Kliknij **Utwórz**.

Harmonogram i warunki rozpoczęcia

Harmonogram

Plan skryptów można skonfigurować tak, by był uruchamiany raz lub wielokrotnie oraz by był uruchamiany zgodnie z harmonogramem lub wyzwalany przez określone zdarzenie.

Dostępne są następujące opcje:

- Uruchom raz
  W przypadku włączenia tej opcji należy skonfigurować datę i godzinę uruchomienia planu.
- Zaplanuj według czasu
  W przypadku włączenia tej opcji można skonfigurować plany skryptów uruchamiane co godzinę, codziennie lub co miesiąc.

© Acronis International GmbH, 2003-2024

Aby harmonogram obowiązywał tylko tymczasowo, zaznacz pole wyboru **Uruchom w podanym okresie**, a następnie skonfiguruj okres, w którym będzie uruchamiany uwzględniony w harmonogramie plan.

- Gdy użytkownik zaloguje się w systemie

  Możesz określić, czy plan skryptów ma być wyzwalany przez zalogowanie się określonego użytkownika, czy zalogowanie się każdego użytkownika.
- Gdy użytkownik wyloguje się z systemu

  Możesz określić, czy plan skryptów ma być wyzwalany przez wylogowanie się określonego użytkownika, czy wylogowanie się każdego użytkownika.
- Podczas uruchamiania systemu
- Gdy system jest wyłączany

  Uwaga
  Ta opcja harmonogramu działa tylko w przypadku skryptów uruchamianych na koncie systemowym.
- Gdy system przechodzi w tryb online

Warunki rozpoczęcia

Warunki rozpoczęcia zapewniają większą elastyczność planowania. W przypadku skonfigurowania wielu warunków plan zostanie uruchomiony dopiero wtedy, gdy wszystkie te warunki zostaną spełnione.

Warunki rozpoczęcia nie obowiązują w przypadku ręcznego uruchomienia planu za pomocą opcji **Uruchom teraz**.

Warunek	Opis
Uruchom tylko wtedy, gdy obciążenie jest w trybie online	Skrypt zostanie uruchomiony, gdy docelowe obciążenie będzie mieć nawiązane połączenie z Internetem.
Użytkownik jest bezczynny	Ten warunek zostaje spełniony, gdy na komputerze uruchamia się wygaszacz ekranu lub komputer zostaje zablokowany.
Użytkownik wylogowany	Dzięki temu warunkowi można opóźnić zaplanowany plan skryptów do momentu wylogowania się użytkownika z docelowego obciążenia.
Mieści się w przedziale czasu	W przypadku tego warunku plan skryptów może zostać uruchomiony tylko w określonym przedziale czasu. Warunku tego można na przykład użyć do ograniczenia warunku **Użytkownik wylogował się**.
Oszczędzaj baterię	Ten warunek pozwala zadbać, aby działanie planu skryptów nie zostało przerwane z powodu niskiego poziomu naładowania baterii. Dostępne są następujące opcje: • Nie uruchamiaj przy zasilaniu z baterii

© Acronis International GmbH, 2003-2024

Warunek	Opis
	Ten plan zostanie uruchomiony tylko wtedy, gdy komputer jest podłączony do źródła zasilania. • Uruchom przy zasilaniu z baterii, jeśli poziom naładowania przekracza Ten plan zostanie uruchomiony, jeśli komputer jest podłączony do źródła zasilania lub poziom naładowania baterii przewyższa określoną wartość.
Nie uruchamiaj przy połączeniu taryfowym	Ten warunek uniemożliwia uruchomienie planu, jeśli docelowe obciążenie uzyskuje dostęp do Internetu za pomocą połączenia taryfowego.
Nie uruchamiaj przy połączeniu z następującymi sieciami Wi-Fi	Ten warunek uniemożliwia uruchomienie planu, jeśli docelowe obciążenie jest połączone z którąkolwiek ze wskazanych sieci bezprzewodowych. Aby skorzystać z tego warunku, należy podać identyfikator SSID zabronionej sieci. Ograniczenie to ma zastosowanie do wszystkich sieci mających w nazwie określony ciąg znaków (wielkość liter jest rozróżniana). Jeśli na przykład wpiszesz `telefon` jako nazwę sieci, plan nie zostanie uruchomiony, jeśli urządzenie będzie podłączone do jednej z następujących sieci: `telefon Joli`, `telefon_wifi` lub `mój_TELEFON_wifi`.
Sprawdź adres IP urządzenia	Ten warunek uniemożliwia uruchomienie planu, jeśli którykolwiek z adresów IP docelowego obciążenia znajduje się w podanym zakresie adresów IP lub poza nim. Dostępne są następujące opcje: • Uruchom, jeśli jest spoza zakresu adresów IP • Uruchom, jeśli jest w zakresie adresów IP Obsługiwane są tylko adresy IPv4.
Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie	Ta opcja umożliwia określenie przedziału czasu, po którym plan zostanie uruchomiony — bez względu na pozostałe warunki. Plan zostanie uruchomiony po spełnieniu pozostałych warunków lub po upływie określonego czasu, w zależności od tego, co nastąpi wcześniej. Ta opcja nie jest dostępna, jeśli plan skryptów skonfigurowano tak, aby został uruchomiony tylko raz.

Zarządzanie docelowymi obciążeniami w ramach planu

Podczas tworzenia planu skryptów lub później można wybrać obciążenia bądź grupy urządzeń, do których ma on zostać zastosowany.

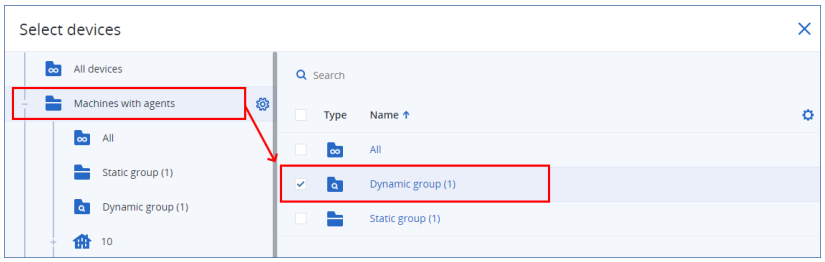
Administratorzy partnerów mogą stosować ten sam plan do obciążeń różnych klientów, a także tworzyć grupy urządzeń zawierające obciążenia różnych klientów. Informacje na temat tworzenia statycznej lub dynamicznej grupy urządzeń na poziomie partnera można znaleźć w sekcji "Karta Urządzenia" (s. 317).

Aby dodać pierwsze obciążenia do planu

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany skryptów**.
2. Kliknij nazwę planu, którego docelowe obciążenia chcesz określić.
3. Kliknij **Dodaj obciążenia**.
4. Wybierz odpowiednie obciążenia lub grupy urządzeń, a następnie kliknij **Dodaj**.

Uwaga
Aby wybrać grupę urządzeń, należy kliknąć jej poziom nadrzędny, a następnie w głównym okienku zaznaczyć pole wyboru obok jej nazwy.

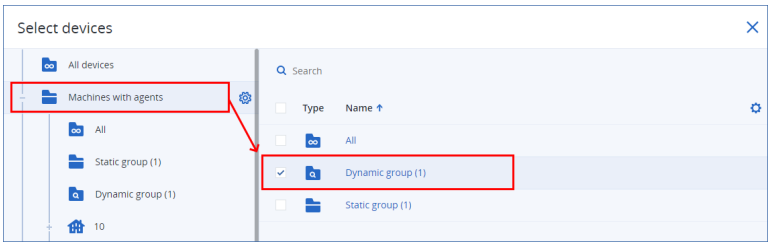


5. Aby zapisać edytowany plan, kliknij **Zapisz**.

Aby zarządzać już istniejącymi obciążeniami w ramach planu

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany skryptów**.
2. Kliknij nazwę planu, którego docelowe obciążenia chcesz zmienić.
3. Kliknij **Zarządzaj obciążeniami**.
   Ekran **Urządzenia** zawiera listę obciążeń, do których obecnie jest stosowany plan skryptów. W przypadku zarządzania więcej niż jednym dzierżawcą obciążenia są sortowane według dzierżawcy.
   - Aby dodać nowe obciążenia lub grupy urządzeń, kliknij **Dodaj**.
     a. Wybierz odpowiednie obciążenia lub grupy urządzeń. Możesz dodać obciążenia pochodzące od wszystkich zarządzanych przez Ciebie dzierżawców.

     Uwaga
     Aby wybrać grupę urządzeń, należy kliknąć jej poziom nadrzędny, a następnie w głównym okienku zaznaczyć pole wyboru obok jej nazwy.

     b. Kliknij **Dodaj**.
   - Aby usunąć obciążenia lub grupy urządzeń, zaznacz je, a następnie kliknij **Usuń**.

© Acronis International GmbH, 2003-2024

4. Kliknij **Gotowe**.
5. Aby zapisać edytowany plan, kliknij **Zapisz**.

Plany na różnych poziomach administracji

Poniższa tabela zawiera zestawienie, które plany są widoczne i dostępne do zarządzania dla administratorów różnych poziomów.

Administrator	Poziom administracji	Plany	Prawa
Administrator partnera	Poziom partnera	Własne plany	Pełny dostęp
		Plany klienta (w tym plany w jednostkach)	Pełny dostęp
		Plany jednostki	Pełny dostęp
	Poziom klienta (dla klientów, którzy są zarządzani przez usługodawcę)	Plany partnera, które są stosowane do obciążeń tego klienta	Tylko do odczytu
		Plany klienta (w tym plany w jednostkach)	Pełny dostęp
		Plany jednostki	Pełny dostęp
	Poziom jednostki (dla klientów, którzy są zarządzani przez usługodawcę)	Plany partnera, które są stosowane do obciążeń tej jednostki	Tylko do odczytu
		Plany klienta, które są stosowane do obciążeń tej jednostki	Tylko do odczytu
		Plany jednostki	Pełny dostęp
Administrator firmy	Poziom klienta	Plany partnera, które są stosowane do obciążeń tego klienta lub jednostki	Tylko do odczytu
		Plany klienta (w tym plany w jednostkach)	Pełny dostęp
		Plany jednostki	Pełny dostęp
	Poziom jednostki	Plany partnera, które są stosowane do obciążeń tej jednostki	Tylko do odczytu
		Plany klienta, które są stosowane do obciążeń tej jednostki	Tylko do odczytu

© Acronis International GmbH, 2003-2024

Administrator	Poziom administracji	Plany	Prawa
		Plany jednostki	Pełny dostęp
Administrator jednostki	Poziom jednostki	Plany partnera, które są stosowane do obciążeń tej jednostki	Tylko do odczytu
		Plany klienta, które są stosowane do obciążeń tej jednostki	Tylko do odczytu
		Plany jednostki	Pełny dostęp

Ważne
Właścicielem planu jest dzierżawca, w ramach którego plan został utworzony. Jeśli więc administrator partnera utworzył plan na poziomie dzierżawcy-klienta, właścicielem tego planu jest dany dzierżawca-klient.

Problemy z kompatybilnością dotyczące planów skryptów

W niektórych przypadkach zastosowanie planu skryptów na obciążeniu może spowodować problemy z kompatybilnością. Można zauważyć następujące problemy z kompatybilnością:

- Niekompatybilny system operacyjny — ten problem jest powodowany nieobsługiwanym systemem operacyjnym obciążenia.
- Nieobsługiwany agent — ten problem występuje, gdy na obciążeniu znajduje się agent ochrony w przestarzałej wersji, który nie obsługuje funkcji Skrypty cybernetyczne.
- Za mały limit — ten problem występuje, gdy dzierżawca ma zbyt mały limit usługi, aby można było ją przypisać do wybranych obciążeń.

Jeśli plan skryptu jest stosowany do maksymalnie 150 indywidualnie wybranych obciążeń, zostanie wyświetlony monit o rozwiązanie istniejących konfliktów przed zapisaniem planu. Aby rozwiązać konflikt, wyeliminuj jego główną przyczynę lub usuń z planu obciążenia, których dotyczy ten konflikt. Aby uzyskać więcej informacji, zobacz "Rozwiązywanie problemów z kompatybilnością dotyczących planów skryptów" (s. 420). W przypadku zapisania planu bez rozwiązania konfliktów zostanie on automatycznie wyłączony dla niekompatybilnych obciążeń i zostaną wyświetlone alerty.

Jeśli plan skryptów zostanie zastosowany do więcej niż 150 obciążeń lub grup urządzeń, zostanie zapisany, a następnie sprawdzony pod kątem kompatybilności. Plan zostanie automatycznie wyłączony w przypadku niekompatybilnych obciążeń, po czym zostaną wyświetlone stosowne alerty.

Rozwiązywanie problemów z kompatybilnością dotyczących planów skryptów

W zależności od przyczyny problemów z kompatybilnością można wykonać różne czynności w celu rozwiązania problemów z kompatybilnością w ramach procesu tworzenia nowego planu skryptów.

© Acronis International GmbH, 2003-2024

Uwaga
W przypadku rozwiązywania problemu ze zgodnością przez usunięcie obciążeń z planu nie można usunąć obciążeń należących do grupy urządzeń.

Aby rozwiązać problemy z kompatybilnością

1. Kliknij **Przejrzyj problemy**.
2. [Aby rozwiązać problemy z kompatybilnością spowodowane przez niekompatybilne systemy operacyjne]
   a. Na karcie **Niekompatybilny system operacyjny** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
3. [Aby rozwiązać problemy z kompatybilnością spowodowane przez nieobsługiwane agenty, usuwając obciążenia z planu]
   a. Na karcie **Nieobsługiwane agenty** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
4. [Aby rozwiązać problemy z kompatybilnością spowodowane przez nieobsługiwane agenty, aktualizując wersje agentów] Kliknij **Przejdź do listy agentów**.

   Uwaga
   Ta opcja jest dostępna wyłącznie dla administratorów klientów.

5. [Aby rozwiązać problemy z kompatybilnością spowodowane za małym limitem przez usunięcie obciążeń z planu]
   a. Na karcie **Za mały limit** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
6. [Aby rozwiązać problemy ze zgodnością spowodowane za małym limitem przez zwiększenie limitu dzierżawcy]

   Uwaga
   Ta opcja jest dostępna wyłącznie dla administratorów partnerów.

   a. Na karcie **Za mały limit** kliknij **Przejdź do portalu zarządzania**.
   b. Zwiększ limit usługi dla klienta.

Szybkie uruchomienie skryptu

Możesz uruchomić skrypt od razu, bez uwzględniania go w planie skryptów. Nie możesz wykonać tej operacji w odniesieniu do więcej niż 150 maszyn, w odniesieniu do maszyn w trybie offline ani w

© Acronis International GmbH, 2003-2024

odniesieniu do grup urządzeń.

Do docelowego obciążenia musi być przypisany limit usług, który obsługuje funkcję Szybkie uruchomienie skryptu, a w przypadku dzierżawcy, do którego należy to obciążenie, musi być włączony pakiet Advanced Management. Automatycznie zostanie przypisany odpowiedni limit usług, jeśli jest on dostępny w ramach danego dzierżawcy.

Uwaga
Możesz używać tylko zatwierdzonych skryptów z sekcji **Repozytorium skryptów** > **Moje skrypty**. Skryptów ze statusem **Testowanie** może używać tylko administrator z rolą **Administrator środowiska cybernetycznego**. Dodatkowe informacje na temat ról można znaleźć w sekcji "Role użytkowników a prawa do funkcji Skrypty cybernetyczne" (s. 400).

Szybkie uruchomienie można rozpocząć następująco:

- Na karcie **Urządzenia**
  Wybierz co najmniej jedno obciążenie, a następnie wybierz skrypt, który ma zostać w odniesieniu do niego uruchomiony.
- Na karcie **Zarządzanie** > **Repozytorium skryptów**
  Wybierz skrypt, a następnie wybierz co najmniej jedno docelowe obciążenie.

Aby uruchomić skrypt na karcie Urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz obciążenie, w odniesieniu do którego chcesz uruchomić skrypt, i kliknij **Chroń**.
3. Kliknij **Szybkie uruchomienie skryptu**.
4. Kliknij **Wybierz skrypt**, wybierz skrypt, którego chcesz użyć, a następnie kliknij **Gotowe**.
5. Wybierz konto, na którym skrypt będzie uruchamiany na docelowym obciążeniu. Dostępne są następujące opcje:
   - Konto systemowe (w systemie macOS jest to konto użytkownika root)
   - Aktualnie zalogowane konto
6. Określ, jak długo skrypt ma być wykonywany na docelowym obciążeniu.
   Jeśli skrypt nie zakończy działania w określonym czasie, operacja skryptów cybernetycznych zakończy się niepowodzeniem.
   Można używać wartości z zakresu od 1 do 1440 minut.
7. [Tylko w przypadku skryptów PowerShell] Skonfiguruj zasady wykonywania programu PowerShell.
   Więcej informacji na temat tych zasad można znaleźć w dokumentacji firmy Microsoft.
8. Kliknij **Uruchom teraz**.

Aby uruchomić skrypt na karcie Repozytorium skryptów

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Repozytorium skryptów**.
2. Wybierz skrypt, który chcesz uruchomić, i kliknij **Szybkie uruchomienie skryptu**.

© Acronis International GmbH, 2003-2024

3. Kliknij **Dodaj obciążenia**, aby wybrać docelowe obciążenia, a następnie kliknij **Dodaj**.
4. Kliknij **Wybierz skrypt**, wybierz skrypt, którego chcesz użyć, a następnie kliknij **Gotowe**.
5. Wybierz konto, na którym skrypt będzie uruchamiany na docelowym obciążeniu. Dostępne są następujące opcje:
   - Konto systemowe (w systemie macOS jest to konto użytkownika root)
   - Aktualnie zalogowane konto
6. Określ, jak długo skrypt ma być wykonywany na docelowym obciążeniu.

   Jeśli skrypt nie zakończy działania w określonym czasie, operacja skryptów cybernetycznych zakończy się niepowodzeniem.

   Można używać wartości z zakresu od 1 do 1440 minut.
7. [Tylko w przypadku skryptów PowerShell] Skonfiguruj zasady wykonywania programu PowerShell.

   Więcej informacji na temat tych zasad można znaleźć w dokumentacji firmy Microsoft.
8. Kliknij **Uruchom teraz**.

© Acronis International GmbH, 2003-2024

Zarządzanie tworzeniem kopii zapasowych oraz odzyskiwaniem obciążeń i plików

Moduł Kopia zapasowa umożliwia tworzenie kopii zapasowych i odzyskiwanie komputerów fizycznych oraz maszyn wirtualnych, plików i baz danych w magazynie lokalnym lub chmurze.

Kopia zapasowa

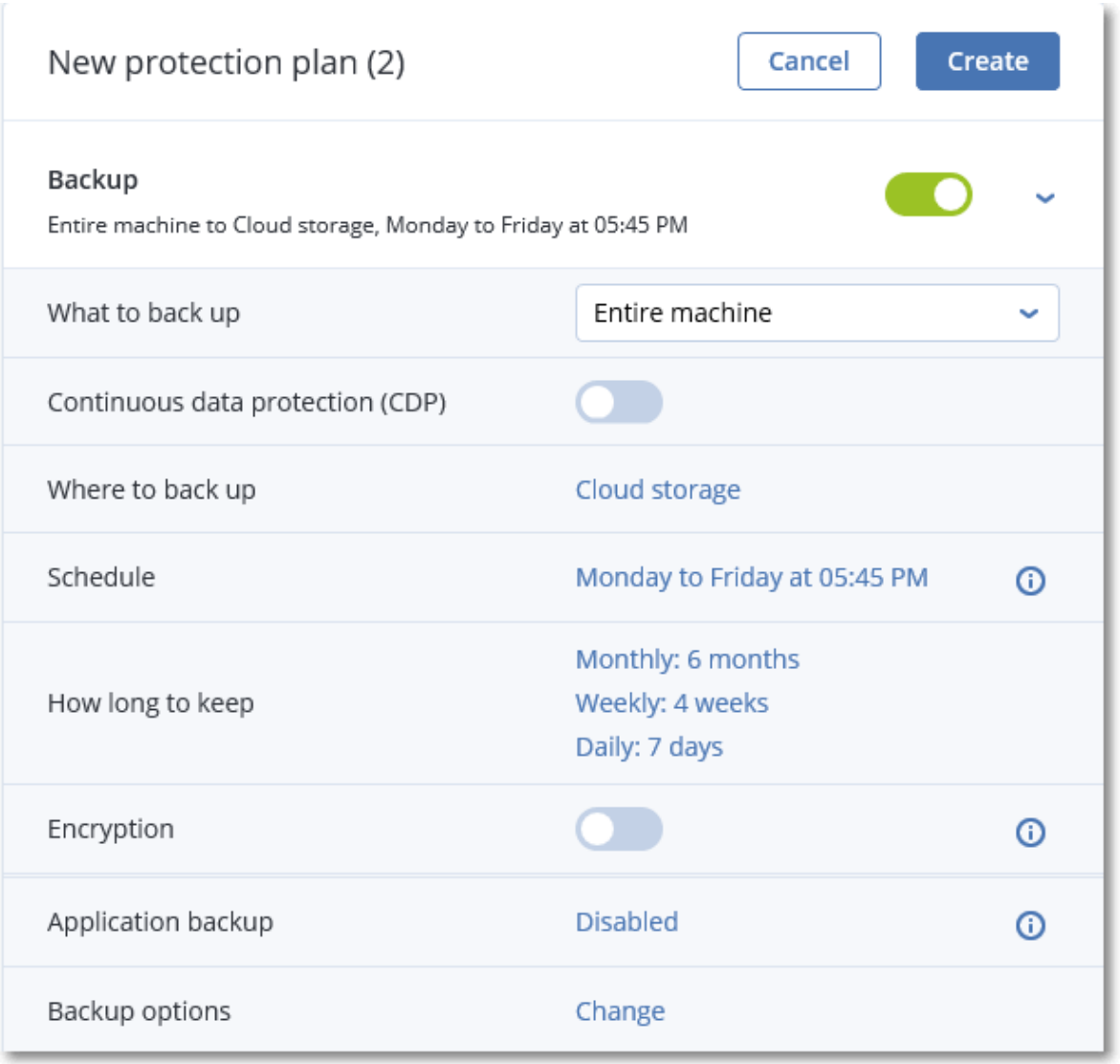
Plan ochrony z włączonym modułem Kopia zapasowa to zestaw reguł określających sposób ochrony konkretnych danych na konkretnym komputerze.

Plan ochrony można zastosować do wielu komputerów — w trakcie jego tworzenia lub później.

Aby utworzyć pierwszy plan ochrony z włączonym modułem Kopia zapasowa

1. Wybierz komputery, których kopie zapasowe chcesz utworzyć.
2. Kliknij **Chroń**.
   Zostaną wyświetlone plany ochrony zastosowane do danego komputera. Jeśli do komputera nie przypisano jeszcze żadnych planów, pojawi się domyślny plan ochrony, który można zastosować. W razie potrzeby można dostosować ustawienia i zastosować ten plan lub utworzyć nowy.
3. Aby utworzyć nowy plan, kliknij **Utwórz plan**. Włącz moduł **Kopia zapasowa** i rozwiń sekcję ustawień.

© Acronis International GmbH, 2003-2024

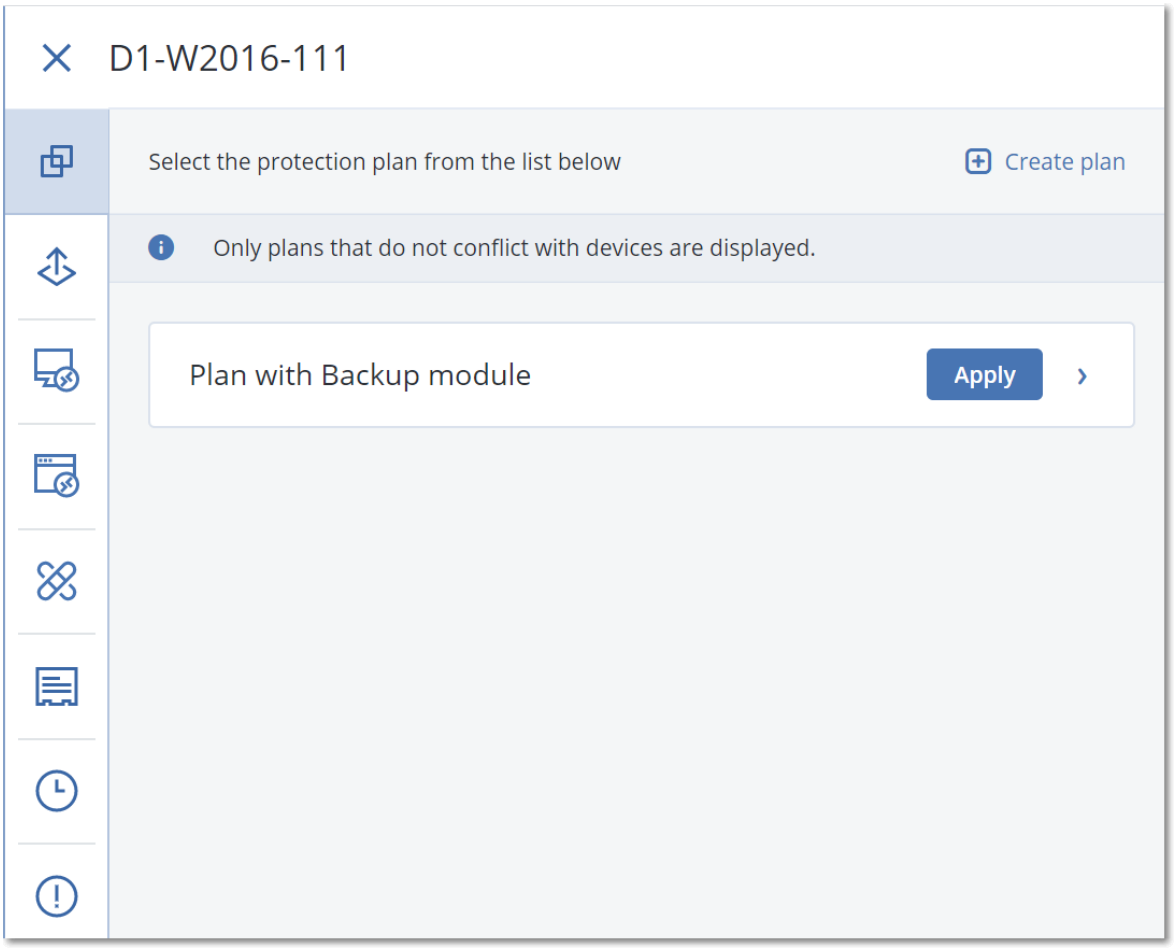


4. [Opcjonalnie] Aby zmienić nazwę planu ochrony, kliknij nazwę domyślną.
5. [Opcjonalnie] Aby zmodyfikować parametry modułu Kopia zapasowa, kliknij odpowiednie ustawienie w panelu planu ochrony.
6. [Optional] Aby zmodyfikować opcje tworzenia kopii zapasowych, kliknij **Zmień** obok pozycji **Opcje tworzenia kopii zapasowych**.
7. Kliknij **Utwórz**.

Aby zastosować już istniejący plan ochrony

1. Wybierz komputery, których kopie zapasowe chcesz utworzyć.
2. Kliknij **Chroń**. Jeśli do wybranych komputerów jest już stosowany wspólny plan ochrony, kliknij **Dodaj plan**.
   W oprogramowaniu zostaną wyświetlone utworzone wcześniej plany ochrony.

© Acronis International GmbH, 2003-2024



3. Wybierz plan ochrony, który chcesz zastosować.
4. Kliknij **Zastosuj**.

Plan ochrony — ściągawka

W poniższej tabeli zestawiono dostępne parametry planów ochrony. Dzięki temu przygotujesz optymalny plan ochrony.

OBIEKTY DO UWZGLĘDNIENIA W KOPII ZAPASOWEJ	ELEMENTY DO UWZGLĘDNIENIA W KOPII ZAPASOWEJ Metody wyboru	MIEJSCE DOCELOWE KOPII ZAPASOWEJ	HARMONOGRAM Schematy tworzenia kopii zapasowych	OKRES PRZECHOWYWANIA
Dyski/woluminy (komputery fizyczne[1])	Wybór bezpośredni Reguły zasad Filtry plików	Chmura Folder lokalny Folder	Zawsze przyrostowa (jednoplikowa) Zawsze pełne	Według wieku kopii zapasowych (jedna reguła na zestaw kopii zapasowych)

[1]Komputer, którego kopie zapasowe są tworzone przez agenta zainstalowanego w systemie operacyjnym.

© Acronis International GmbH, 2003-2024

		sieciowy NFS* Secure Zone**	Tygodniowe pełne, dzienne przyrostowe Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe (GFS) Niestandardowe (P-D-P)	Według liczby kopii zapasowych Według łącznego rozmiaru kopii zapasowych*** Zachowaj w nieskończoność
Dyski/woluminy (maszyny wirtualne[1])	Reguły zasad Filtry plików	Chmura Folder lokalny Folder sieciowy NFS*		
Pliki (tylko komputery fizyczne[2])	Wybór bezpośredni Reguły zasad Filtry plików	Chmura Folder lokalny Folder sieciowy NFS* Secure Zone**	Zawsze przyrostowa (jednoplikowa) Zawsze pełne Tygodniowe pełne, dzienne przyrostowe Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe (GFS) Niestandardowe (P-D-P)	
Konfiguracja ESXi	Wybór bezpośredni	Folder lokalny Folder sieciowy NFS*		
Witryny internetowe (pliki i bazy danych MySQL)	Wybór bezpośredni	Chmura	—	

[1]Maszyna wirtualna, której kopie zapasowe są tworzone na poziomie hiperwizora przez agenta zewnętrznego, takiego jak agent dla VMware lub agent dla Hyper-V. Maszyna wirtualna zawierająca agenta jest z perspektywy tworzenia kopii zapasowych traktowana jak komputer fizyczny.
[2]Komputer, którego kopie zapasowe są tworzone przez agenta zainstalowanego w systemie operacyjnym.

© Acronis International GmbH, 2003-2024

<table>
<tr><td colspan="2">Stan systemu</td><td rowspan="3">Wybór bezpośredni</td><td>Chmura
Folder lokalny
Folder sieciowy</td><td>Zawsze pełne
Tygodniowe pełne, dzienne przyrostowe
Niestandardowe (P-P)
Zawsze przyrostowa (jednoplikowa) — tylko w przypadku baz danych SQL</td><td rowspan="8"></td></tr>
<tr><td colspan="2">Bazy danych SQL</td></tr>
<tr><td colspan="2">Bazy danych programu Exchange</td></tr>
<tr><td rowspan="8">Microsoft 365</td><td>Skrzynki pocztowe
(lokalny agent dla usługi Microsoft 365)</td><td>Wybór bezpośredni</td><td>Chmura
Folder lokalny
Folder sieciowy</td></tr>
<tr><td>Skrzynki pocztowe
(chmurowy agent dla usługi Microsoft 365)</td><td rowspan="3">Wybór bezpośredni</td><td rowspan="5">Chmura</td><td rowspan="4">Do 6 kopii zapasowych dziennie</td></tr>
<tr><td>Foldery publiczne</td></tr>
<tr><td>Teams</td></tr>
<tr><td>Pliki w usłudze OneDrive</td><td rowspan="2">Wybór bezpośredni
Reguły zasad</td></tr>
<tr><td>Dane programu SharePoint Online</td></tr>
<tr><td rowspan="3">Google Workspace</td><td>Skrzynki pocztowe Gmail</td><td>Wybór bezpośredni</td><td rowspan="3">Chmura</td><td rowspan="3">Do 6 kopii zapasowych dziennie</td></tr>
<tr><td>Pliki z dysku Google</td><td rowspan="2">Wybór bezpośredni
Reguły zasad</td></tr>
<tr><td>Pliki z Dysku współdzielonego</td></tr>
</table>

***** W systemie Windows tworzenie kopii zapasowych w udziałach NFS jest niedostępne.

** Na komputerze z systemem Mac nie można utworzyć strefy Secure Zone.

*** Ustawienie **Według łącznego rozmiaru kopii zapasowych** jest niedostępne w przypadku schematu tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** ani podczas tworzenia kopii zapasowej w chmurze.

© Acronis International GmbH, 2003-2024

Wybieranie danych do uwzględnienia w kopii zapasowej

Wybieranie całego komputera

W kopii zapasowej całego komputera są uwzględniane wszystkie jego dyski niewymienne. Więcej informacji o kopii zapasowej dysku można znaleźć w sekcji "Wybieranie dysków lub woluminów" (s. 429).

Ograniczenia

- Kopie zapasowe na poziomie dysku nie są obsługiwane w przypadku zablokowanych zaszyfrowanych woluminów APFS. W przypadku tworzenia kopii zapasowej całej maszyny takie woluminy są pomijane.
- Folder główny OneDrive jest domyślnie wykluczany z operacji tworzenia kopii zapasowych. W przypadku wybrania określonych plików i folderów OneDrive będą one uwzględniane w kopii zapasowej. Pliki, które nie są dostępne na urządzeniu, będą miały nieprawidłową zawartość w zestawie kopii zapasowych.

Wybieranie dysków lub woluminów

Kopia zapasowa na poziomie dysku zawiera kopię dysku lub woluminu w postaci spakowanej. Z kopii zapasowej na poziomie dysku można odzyskiwać dyski, woluminy, foldery i pliki.

Można wybrać dyski lub woluminy do uwzględnienia w kopii zapasowej w przypadku wybranych obciążeń w planie ochrony (wybór bezpośredni) lub skonfigurować reguły na potrzeby wielu obciążeń. Ponadto można wykluczyć określone pliki z kopii zapasowej lub uwzględnić w niej tylko konkretne pliki, konfigurując filtry plików. Aby uzyskać więcej informacji, zobacz "Filtry plików (uwzględniające/wykluczające)" (s. 494).

Aby wybrać dyski lub woluminy

Wybór bezpośredni

Wybór bezpośredni jest dostępny tylko w przypadku komputerów fizycznych.

1. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Dyski/woluminy**.
2. Kliknij **Elementy uwzględniane w kopii zapasowej**.
3. W polu **Wybierz elementy do uwzględnienia w kopii zapasowej** wybierz **Bezpośrednio**.
4. W przypadku każdego obciążenia objętego planem ochrony zaznacz pola wyboru obok dysków lub woluminów, które mają zostać uwzględnione w kopii zapasowej.
5. Kliknij **Gotowe**.

Za pomocą reguł

© Acronis International GmbH, 2003-2024

1. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Dyski/woluminy**.
2. Kliknij **Elementy uwzględniane w kopii zapasowej**.
3. W polu **Wybierz elementy do uwzględnienia w kopii zapasowej** wybierz **Użycie reguł zasad**.
4. Wybierz dowolne z gotowych reguł, wpisz własne reguły lub skorzystaj z obu tych możliwości.
   Dodatkowe informacje na temat dostępnych reguł można znaleźć w sekcji "Reguły dotyczące dysków i woluminów" (s. 432).
   Reguły będą stosowane do wszystkich obciążeń objętych planem ochrony.
   Jeśli żadna z określonych reguł nie może zostać zastosowana do obciążenia, tworzenie kopii zapasowej tego obciążenia zakończy się niepowodzeniem.
5. Kliknij **Gotowe**.

Ograniczenia

- Kopie zapasowe na poziomie dysku nie są obsługiwane w przypadku zablokowanych zaszyfrowanych woluminów APFS. W przypadku tworzenia kopii zapasowej całej maszyny takie woluminy są pomijane.
- Folder główny OneDrive jest domyślnie wykluczany z operacji tworzenia kopii zapasowych. W przypadku wybrania określonych plików i folderów OneDrive będą one uwzględniane w kopii zapasowej. Pliki, które nie są dostępne na urządzeniu, będą miały nieprawidłową zawartość w zestawie kopii zapasowych.
- Istnieje możliwość utworzenia kopii zapasowej dysków podłączonych do komputera fizycznego za pośrednictwem protokołu iSCSI. Jeśli jednak do tworzenia kopii zapasowej dysków podłączonych za pośrednictwem protokołu iSCSI jest używany agent dla VMware lub agent dla Hyper-V, występują pewne ograniczenia. Aby uzyskać więcej informacji, zobacz "Ograniczenia" (s. 34).

Co zawiera kopia zapasowa dysku lub woluminu?

Utworzenie kopii zapasowej dysku lub woluminu polega na zapisaniu całego **systemu plików** dysku lub woluminu wraz z wszystkimi informacjami potrzebnymi do uruchomienia systemu operacyjnego. Z takich kopii zapasowych można odzyskać całe dyski lub woluminy, jak również poszczególne pliki lub foldery.

Jeśli jest włączona opcja **„sektor po sektorze" (tryb „surowych" danych)** kopii zapasowej, w kopii zapasowej dysku są zapisywane wszystkie jego sektory. Operacja kopiowania „sektor po sektorze" pozwala tworzyć kopie zapasowe dysków zawierających nierozpoznane lub nieobsługiwane systemy plików oraz dane w innych zastrzeżonych formatach.

Windows

Kopia zapasowa woluminu zawiera wszystkie pliki i foldery wybranego woluminu niezależnie od ich atrybutów (w tym pliki ukryte i systemowe), rekord startowy, tablicę FAT (o ile istnieje), katalog główny i zerową ścieżkę dysku twardego z głównym rekordem startowym (MBR).

© Acronis International GmbH, 2003-2024

Kopia zapasowa dysku zawiera wszystkie woluminy wybranego dysku (w tym woluminy ukryte, takie jak partycje konserwacyjne producenta) oraz ścieżkę zerową głównego rekordu rozruchowego.

Kopia zapasowa dysku ani woluminu (ani kopia na poziomie plików) *nie* zawiera następujących elementów:

- Plik wymiany (pagefile.sys) i plik z zawartością pamięci RAM komputera przechodzącego w stan hibernacji (hiberfil.sys). Po odzyskaniu danych pliki te zostaną ponownie utworzone w odpowiednim miejscu z zerowym rozmiarem.
- Jeśli kopia zapasowa jest tworzona w systemie operacyjnym (inaczej niż w przypadku tworzenia kopii zapasowej na nośnik startowy lub tworzenia kopii zapasowej maszyn wirtualnych z poziomu hiperwizora):
  - Magazyn kopii w tle systemu Windows. Ścieżkę do tego magazynu określa wartość rejestru **VSS Default Provider**, która znajduje się w kluczu rejestru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Oznacza to, że od wersji Windows Vista w systemach operacyjnych Windows nie tworzy się kopii zapasowych punktów przywracania systemu.
  - Jeśli jest włączona opcja tworzenia kopii zapasowych **Usługa kopiowania woluminów w tle (VSS)**, obejmuje to pliki i foldery określone w kluczu rejestru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**.

Linux

Kopia zapasowa woluminu zawiera wszystkie pliki i katalogi wybranego woluminu niezależnie od ich atrybutów, rekord startowy oraz superblok systemu plików.

Kopia zapasowa dysku zawiera wszystkie woluminy dysku oraz ścieżkę zerową z głównym rekordem rozruchowym.

Mac

Kopia zapasowa dysku lub woluminu przechowuje wszystkie pliki i katalogi wybranego dysku lub woluminu, a także opis układu woluminu.

Wykluczone są następujące elementy:

- Metadane systemu, takie jak dziennik systemu plików indeks funkcji Spotlight
- Kosz
- Kopie zapasowe programu Time Machine

Kopie zapasowe dysków i woluminów komputera Mac są tworzone fizycznie na poziomie pliku. Można odzyskać kopię zapasową dysku lub woluminu bez systemu operacyjnego, ale nie jest dostępny tryb kopii zapasowej sektor po sektorze.

© Acronis International GmbH, 2003-2024

Reguły dotyczące dysków i woluminów

Po wybraniu dysków lub woluminów do uwzględnienia w kopii zapasowej można użyć następujących reguł — odpowiednio do systemu operacyjnego chronionego obciążenia.

Windows

- `[All Volumes]` powoduje wybranie wszystkich woluminów dostępnych na komputerze.
- Litera dysku (na przykład `C:\`) powoduje wybranie woluminu z określoną literą dysku.
- `[Fixed Volumes (physical machines)]` powoduje wybranie wszystkich woluminów dostępnych na komputerze fizycznym, z wyjątkiem nośników wymiennych. Woluminy stałe obejmują woluminy na urządzeniach SCSI, ATAPI, ATA, SSA, SAS i SATA oraz macierzy RAID.
- `[BOOT+SYSTEM]` powoduje wybranie woluminu systemowego i startowych. Jest to minimalna kombinacja, z której można odzyskać system operacyjny.
- `[Disk 1]` powoduje wybranie pierwszego dysku komputera i obejmuje wszystkie woluminy na tym dysku. Aby wybrać inny dysk, wpisz odpowiedni numer.

Linux

- `[All Volumes]` powoduje wybranie wszystkich zamontowanych woluminów dostępnych na komputerze.
- `/dev/hda1` powoduje wybranie pierwszego woluminu pierwszego dysku twardego IDE.
- `/dev/sda1` powoduje wybranie pierwszego woluminu pierwszego dysku twardego SCSI.
- `/dev/md1` powoduje wybranie pierwszego dysku twardego programowej macierzy RAID.
- Aby wybrać inne woluminy standardowe, określ `/dev/xdyN`, gdzie:
  - „x” odpowiada typowi dysku
  - „y” odpowiada numerowi dysku (a w przypadku pierwszego dysku, b w przypadku drugiego dysku itd.)
  - „N” oznacza numer woluminu
- Aby wybrać wolumin logiczny, podaj jego ścieżkę, która pojawi się po uruchomieniu polecenia `ls /dev/mapper` na koncie użytkownika root.

  Na przykład:

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  Zostaną wyświetlone dwa woluminy logiczne — `lv1` i `lv2` — należące do grupy woluminów `vg_1`. Aby utworzyć kopię zapasową tych woluminów, wprowadź:

  `/dev/mapper/vg_1-lv1`
  `/dev/mapper/vg-l-lv2`

macOS

© Acronis International GmbH, 2003-2024

- `[All Volumes]` powoduje wybranie wszystkich zamontowanych woluminów dostępnych na komputerze.
- `[Disk 1]` powoduje wybranie pierwszego dysku komputera i obejmuje wszystkie woluminy na tym dysku. Aby wybrać inny dysk, wprowadź odpowiedni numer.

Wybieranie plików lub folderów

Użyj kopii zapasowej na poziomie plików, aby chronić tylko określone dane, na przykład pliki w bieżącym projekcie. Kopie zapasowe na poziomie plików są mniejsze niż kopie zapasowe na poziomie dysku i zapewniają oszczędność miejsca w pamięci masowej.

Ważne
Z kopii zapasowej na poziomie plików nie można odzyskać systemu operacyjnego.

Można wybrać pliki i foldery do uwzględnienia w kopii zapasowej w przypadku wybranych obciążeń w planie ochrony (wybór bezpośredni) lub skonfigurować reguły na potrzeby wielu obciążeń. Ponadto można wykluczyć określone pliki z kopii zapasowej lub uwzględnić w niej tylko konkretne pliki, konfigurując filtry plików. Aby uzyskać więcej informacji, zobacz "Filtry plików (uwzględniające/wykluczające)" (s. 494).

Aby wybrać pliki lub foldery

Wybór bezpośredni

1. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Pliki/foldery**.
2. W polu **Elementy uwzględniane w kopii zapasowej** kliknij **Określ**.
3. W polu **Wybierz elementy do uwzględnienia w kopii zapasowej** wybierz **Bezpośrednio**.
4. Wskaż pliki lub foldery do uwzględnienia w kopii zapasowej w przypadku każdego obciążenia w planie ochrony.
   a. Kliknij **Wybierz pliki i foldery**.
   b. Kliknij **Folder lokalny** lub **Folder sieciowy**.
      Foldery sieciowe muszą być dostępne z wybranego komputera.
      W przypadku wybrania źródła **Folder sieciowy** można tworzyć kopie zapasowe danych zapisanych w sieciowej pamięci masowej (NAS), na przykład na urządzeniach NetApp. Obsługiwane są urządzenia NAS każdego producenta.
   c. W drzewie folderów przejdź do wymaganych plików lub folderów.
      Możesz też podać ścieżkę do nich, a następnie kliknąć przycisk strzałki.
   d. [W przypadku folderów udostępnionych] Po wyświetleniu monitu podaj poświadczenia dostępu do folderu udostępnionego.
      Tworzenie kopii zapasowych folderów z dostępem anonimowym nie jest obsługiwane.
   e. Wybierz wymagane pliki i foldery.
   f. Kliknij **Gotowe**.

Za pomocą reguł

© Acronis International GmbH, 2003-2024

1. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Pliki/foldery**.
2. W polu **Elementy uwzględniane w kopii zapasowej** kliknij **Określ**.
3. W polu **Wybierz elementy do uwzględnienia w kopii zapasowej** wybierz **Użycie reguł zasad**.
4. Wybierz dowolne z gotowych reguł, wpisz własne reguły lub skorzystaj z obu tych możliwości.
   Dodatkowe informacje na temat dostępnych reguł można znaleźć w sekcji "Reguły dotyczące plików i folderów" (s. 434).
   Reguły będą stosowane do wszystkich obciążeń objętych planem ochrony.
   Jeśli żadna z określonych reguł nie może zostać zastosowana do obciążenia, tworzenie kopii zapasowej tego obciążenia zakończy się niepowodzeniem.
5. Kliknij **Gotowe**.

Ograniczenia

- Pliki i foldery można wybierać w przypadku tworzenia kopii zapasowych komputerów fizycznych lub maszyn wirtualnych, na których jest zainstalowany agent (tworzenie kopii zapasowych przy użyciu agenta). Kopie zapasowe na poziomie plików nie są dostępne w przypadku maszyn wirtualnych, których kopie zapasowe są tworzone w trybie bezagentowym. Dodatkowe informacje o różnicach między tymi typami kopii zapasowych można znaleźć w sekcji "Tworzenie kopii zapasowych przy użyciu agenta i bezagentowe" (s. 66).
- Folder główny OneDrive jest domyślnie wykluczany z operacji tworzenia kopii zapasowych. W przypadku wybrania określonych plików i folderów OneDrive będą one uwzględniane w kopii zapasowej. Pliki, które nie są dostępne na urządzeniu, będą miały nieprawidłową zawartość w zestawie kopii zapasowych.
- Istnieje możliwość utworzenia kopii zapasowej plików i folderów znajdujących się na dyskach podłączonych do komputera fizycznego za pośrednictwem protokołu iSCSI. Jeśli do tworzenia kopii zapasowej danych z dysków podłączonych za pośrednictwem protokołu iSCSI jest używany agent dla VMware lub agent dla Hyper-V, występują pewne ograniczenia.

Reguły dotyczące plików i folderów

Po wybraniu plików lub folderów do uwzględnienia w kopii zapasowej można użyć następujących reguł — odpowiednio do systemu operacyjnego chronionego obciążenia.

Windows

- Pełna ścieżka do pliku lub folderu. Na przykład `D:\Praca\Tekst.doc` lub `C:\Windows`.
- Gotowe reguły:
  - `[All Files]` powoduje wybranie wszystkich plików we wszystkich woluminach komputera.
  - `[All Profiles Folder]` powoduje wybranie folderu, w którym znajdują się wszystkie profile użytkowników. Na przykład `C:\Users` lub `C:\Documents and Settings`.
- Zmienne środowiskowe:
  - `%ALLUSERSPROFILE%` powoduje wybranie folderu, w którym znajdują się wspólne dane wszystkich profili użytkowników. Na przykład `C:\ProgramData` lub `C:\Documents and Settings\All Users`.

© Acronis International GmbH, 2003-2024

- `%PROGRAMFILES%` powoduje wybranie folderu `Program Files`. Na przykład `C:\Program Files`.
- `%WINDIR%` powoduje wybranie folderu `Windows`. Na przykład `C:\Windows`.

Można korzystać z innych zmiennych środowiskowych lub łączyć zmienne środowiskowe i tekst. Na przykład w celu wybrania folderu Java w folderze Program Files wpisz: `%PROGRAMFILES%\Java`.

Linux

- Pełna ścieżka pliku lub katalogu.

  Na przykład w celu utworzenia kopii zapasowej pliku `plik.txt` znajdującego się na woluminie `/dev/hda3` zamontowanym w lokalizacji `/home/usr/docs` określ ścieżkę `/dev/hda3/plik.txt` lub `/home/usr/docs/plik.txt`.
- Gotowe reguły:
  - `[All Profiles Folder]` powoduje wybranie folderu `/home`. Domyślnie w folderze tym są przechowywane wszystkie profile użytkowników.
  - `/home` powoduje wybranie katalogu głównego zwykłych użytkowników.
  - `/root` powoduje wybranie katalogu głównego użytkownika root.
  - `/usr` powoduje wybranie katalogu wszystkich programów związanych z użytkownikami.
  - `/etc` powoduje wybranie katalogu plików konfiguracyjnych systemu.

macOS

- Pełna ścieżka pliku lub katalogu.

  Na przykład:
  - Aby uwzględnić w kopii zapasowej plik `plik.txt` z pulpitu użytkownika, określ ścieżkę `/Users/<nazwa użytkownika>/Desktop/plik.txt`.
  - Aby uwzględnić w kopii zapasowej folder `Pulpit`, `Dokumenty` lub `Pobrane` użytkownika, wpisz ścieżkę `/Users/<nazwa użytkownika>/Desktop`, `/Users/<nazwa użytkownika>/Documents` lub `/Users/<nazwa użytkownika>/Downloads`.
  - Aby uwzględnić w kopii zapasowej foldery macierzyste wszystkich użytkowników, którzy mają konto na danym komputerze, określ ścieżkę `/Users`.
  - Aby uwzględnić w kopii zapasowej folder, w którym są zainstalowane aplikacje, wpisz `/Applications`.
- Gotowe reguły
  - `[All Profiles Folder]` powoduje wybranie folderu `/Users`. Domyślnie w folderze tym są przechowywane wszystkie profile użytkowników.

© Acronis International GmbH, 2003-2024

Wybieranie stanu systemu

Uwaga
Kopia zapasowa stanu systemu jest dostępna tylko w przypadku komputerów z systemem Windows 7 lub nowszym, na których jest zainstalowany agent dla systemu Windows. Kopia zapasowa stanu systemu nie jest dostępna w przypadku maszyn wirtualnych, których kopie zapasowe są tworzone na poziomie hiperwizora (bezaganetowe tworzenie kopii zapasowej).

Aby utworzyć kopię zapasową stanu systemu, w polu **Elementy uwzględniane w kopii zapasowej** wybierz **Stan systemu**.

Kopia zapasowa stanu systemu zawiera następujące pliki:

- Konfiguracja Harmonogramu zadań
- Magazyn metadanych usługi VSS
- Informacje konfiguracyjne licznika wydajności
- Usługa MSSearch
- Usługa inteligentnego transferu w tle
- Rejestr
- Instrumentacja zarządzania Windows
- Baza danych rejestracji klas usług składowych

Wybieranie konfiguracji ESXi

Kopia zapasowa konfiguracji hosta ESXi umożliwia odzyskanie hosta ESXi na komputer bez systemu operacyjnego. Operacja odzyskiwania jest realizowana z poziomu nośnika startowego.

Maszyny wirtualne działające na hoście nie są uwzględniane w kopii zapasowej. Można jednak osobno tworzyć ich kopie zapasowe i osobno je odzyskiwać.

Kopia zapasowa konfiguracji hosta ESXi obejmuje:

- Program ładujący oraz partycje banku startowego hosta
- Stan hosta (konfigurację sieci wirtualnej i pamięci masowej, klucze SSL, ustawienia sieci serwera oraz informacje o użytkownikach lokalnych)
- Rozszerzenia i poprawki zainstalowane lub przygotowane na hoście
- Plik dzienników

Wymagania wstępne

- W polu **Profil zabezpieczeń** konfiguracji hosta ESXi musi być włączony protokół SSH.
- Trzeba znać hasło do konta „root” na hoście ESXi.

© Acronis International GmbH, 2003-2024

Ograniczenia

- Kopie zapasowe konfiguracji ESXi nie są obsługiwane w przypadku hostów z VMware ESXi w wersji 7.0 lub nowszej.
- Konfiguracji ESXi nie można uwzględnić w kopii zapasowej w chmurze.

Aby wybrać konfigurację ESXi

1. Kliknij **Urządzenia** > **Wszystkie urządzenia**, a następnie wybierz hosty ESXi, które chcesz uwzględnić w kopii zapasowej.
2. Kliknij **Chroń**.
3. W obszarze **Elementy uwzględniane w kopii zapasowej** zaznacz **Konfiguracja ESXi**.
4. W polu **Hasło do konta „root" ESXi** określ hasło do konta „root" na każdym z wybranych hostów lub zastosuj jedno hasło do wszystkich hostów.

Ciągła ochrona danych

Moduł Ciągła ochrona danych wchodzi w skład pakietu Zaawansowane tworzenie kopii zapasowych. Odpowiada on za tworzenie kopii zapasowych krytycznych danych, gdy tylko zajdzie w nich jakaś zmiana, dzięki czemu żadne zmiany nie zostaną utracone w razie awarii systemu między dwiema zaplanowanymi operacjami tworzenia kopii zapasowej. Ciągłą ochronę danych można skonfigurować w przypadku takich danych jak:

- Pliki lub foldery w określonych lokalizacjach
- Pliki modyfikowane przez określone aplikacje

Ciągła ochrona danych jest obecnie obsługiwana tylko w przypadku systemu plików NTFS i następujących systemów operacyjnych:

- Komputer stacjonarny: Windows 7 lub nowszy
- Serwer: Windows Server 2008 R2 lub nowszy

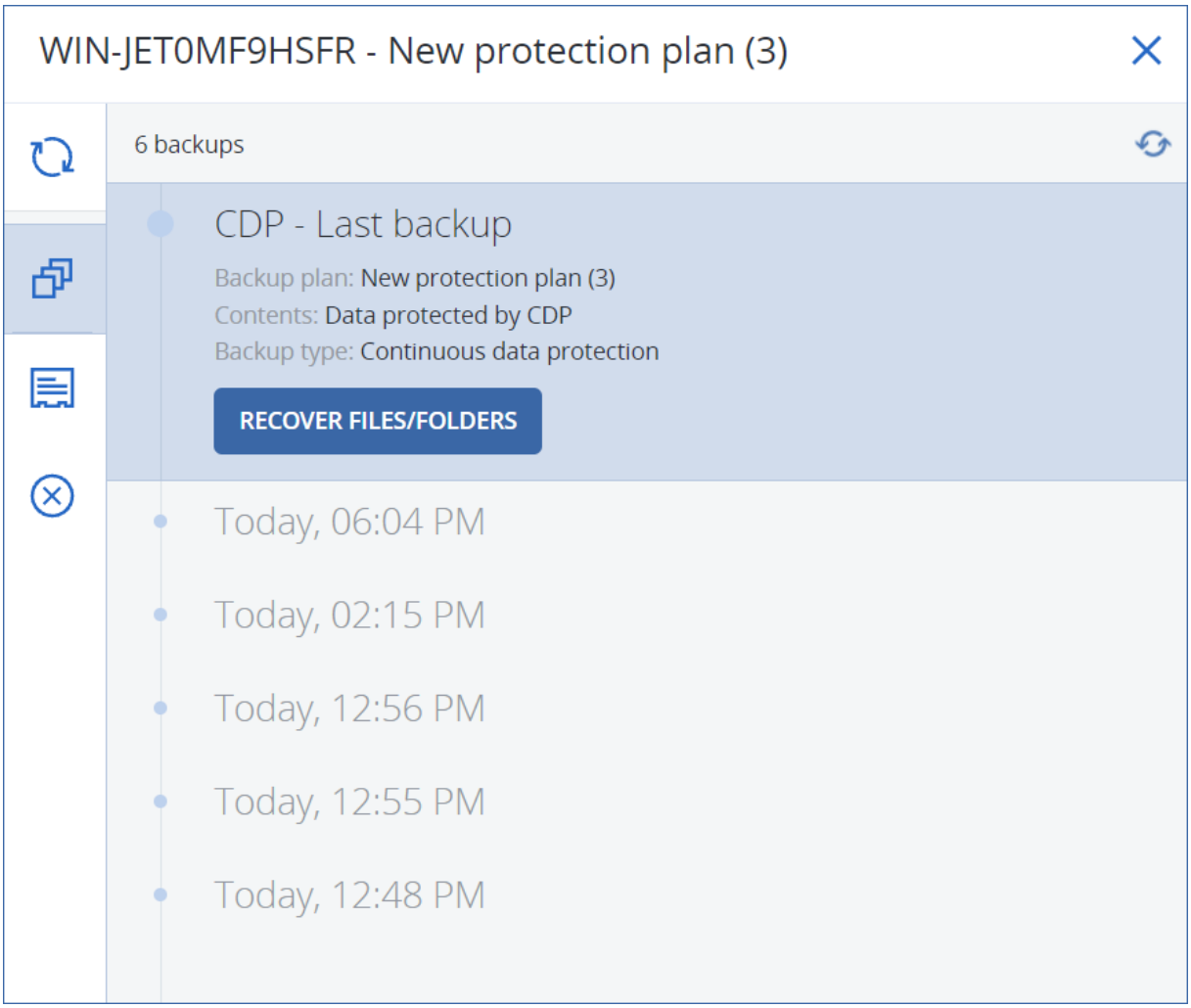
Obsługiwane są tylko foldery lokalne. Folderów sieciowych nie można wybrać do objęcia ciągłą ochroną danych.

Ciągła ochrona danych nie jest zgodna z opcją **Kopia zapasowa aplikacji**.

Sposób działania

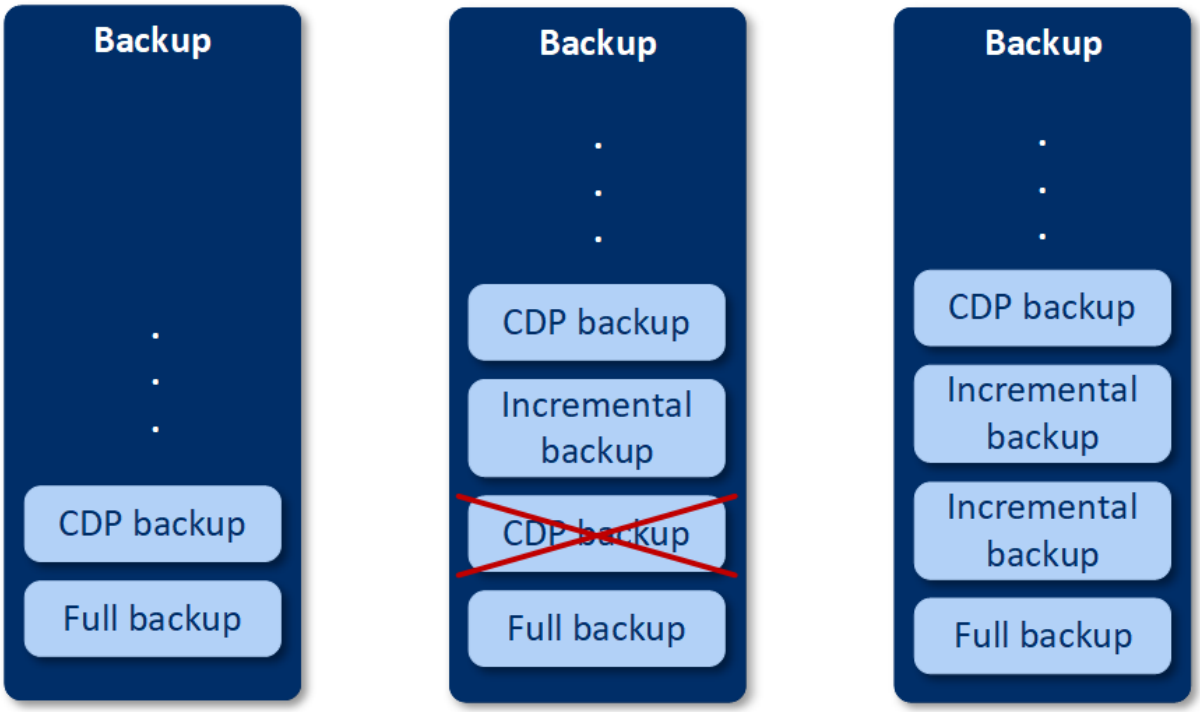
Zmiany w plikach i folderach śledzone przez funkcję Ciągła ochrona danych są niezwłocznie zapisywane w specjalnej kopii zapasowej CDP. W zestawie kopii zapasowych znajduje się tylko jedna kopia zapasowa CDP i zawsze jest to kopia najnowsza.

© Acronis International GmbH, 2003-2024



Gdy się zaczyna zaplanowana operacja tworzenia zwykłej kopii zapasowej, ciągła ochrona danych zostaje wstrzymana, ponieważ najnowsze dane zostaną uwzględnione w zaplanowanej kopii zapasowej. Po zakończeniu tworzenia zaplanowanej kopii zapasowej ciągła ochrona danych zostaje wznowiona, stara kopia zapasowa CDP zostaje usunięta, a w jej miejsce jest tworzona nowa. W związku z tym kopia zapasowa CDP zawsze jest najnowszą kopią w zestawie kopii zapasowych i zawiera tylko najnowszy stan śledzonych plików lub folderów.

© Acronis International GmbH, 2003-2024



Jeśli podczas tworzenia zwykłej kopii zapasowej dojdzie do awarii komputera, ciągła ochrona danych zostanie automatycznie wznowiona po ponownym uruchomieniu komputera i zostanie utworzona kopia zapasowa CDP na podstawie ostatniej pomyślnie utworzonej zaplanowanej kopii zapasowej.

Ciągła ochrona danych wymaga, aby przed kopią zapasową CDP została utworzona co najmniej jedna zwykła kopia zapasowa. Dlatego przy pierwszym uruchomieniu planu ochrony obejmującego ciągłą ochronę danych jest tworzona pełna kopia zapasowa, a następnie niezwłocznie jest dodawana kopia zapasowa CDP. W przypadku włączenia opcji **Ciągła ochrona danych** w ramach już istniejącego planu ochrony kopia zapasowa CDP jest dodawania do już istniejącego zestawu kopii zapasowych.

Uwaga
Moduł Ciągła ochrona danych jest domyślnie włączony w przypadku planów ochrony utworzonych na karcie **Urządzenia**, jeśli usługa Zaawansowane tworzenie kopii zapasowych jest włączona dla użytkownika i w przypadku wybranych komputerów nie są używane inne funkcje usługi Zaawansowane tworzenie kopii zapasowych. Jeśli dla wybranego komputera już istnieje plan z modułem Ciągła ochrona danych, moduł ten nie będzie domyślnie włączany dla tego urządzenia w nowo tworzonych planach.
Moduł Ciągła ochrona danych nie jest domyślnie włączony w przypadku planów tworzonych dla grup urządzeń.

Obsługiwane źródła danych

Ciągłą ochronę danych można skonfigurować w przypadku następujących źródeł danych:

© Acronis International GmbH, 2003-2024

- Cały komputer
- Dyski/woluminy
- Pliki/foldery

Po wybraniu źródła danych w sekcji **Elementy uwzględniane w kopii zapasowej** w planie ochrony w sekcji **Elementy do objęcia ciągłą ochroną** wybierz pliki, foldery lub aplikacje do objęcia ciągłą ochroną danych. Dodatkowe informacje na temat konfigurowania ciągłej ochrony danych można znaleźć w sekcji "Konfigurowanie operacji tworzenia kopii zapasowych CDP" (s. 440).

Obsługiwane lokalizacje docelowe

Ciągłą ochronę danych można skonfigurować w przypadku następujących lokalizacji docelowych:

- Folder lokalny
- Folder sieciowy
- Chmura
- Acronis Cyber Infrastructure
- Lokalizacja zdefiniowana za pomocą skryptu

Uwaga
Za pomocą skryptu można zdefiniować tylko wymienione wyżej lokalizacje.

Konfigurowanie operacji tworzenia kopii zapasowych CDP

Istnieje możliwość skonfigurowania ciągłej ochrony danych w module **Kopia zapasowa** planu ochrony. Dodatkowe informacje na temat tworzenia planu ochrony można znaleźć w sekcji "Tworzenie planu ochrony" (s. 222).

Aby skonfigurować ustawienia ciągłej ochrony danych

1. W module **Kopia zapasowa** planu ochrony włącz przełącznik **Ciągła ochrona danych (CDP)**.
   Przełącznik ten jest dostępny tylko w przypadku następujących źródeł danych:
   - Cały komputer
   - Dyski/woluminy
   - Pliki/foldery
2. W polu **Elementy do objęcia ciągłą ochroną** skonfiguruj ciągłą ochronę danych dla elementów **Aplikacje**, **Pliki/foldery** lub obu tych typów elementów.
   - Kliknij **Aplikacje**, aby skonfigurować kopie zapasowe CDP plików zmodyfikowanych przez określone aplikacje.
     Możesz wybrać aplikacje z gotowych kategorii lub dodać inne aplikacje, określając ścieżki do ich plików wykonywalnych, na przykład:

 © Acronis International GmbH, 2003-2024

- `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
- `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

- Kliknij **Pliki/foldery**, aby skonfigurować kopie zapasowe CDP plików znajdujących się w określonych lokalizacjach.

  Lokalizacje te można definiować za pomocą reguł wyboru lub przez bezpośrednie zaznaczanie plików i folderów.

  - [W przypadku wszystkich komputerów] Aby utworzyć regułę wyboru, użyj pola tekstowego.

    Możesz użyć pełnych ścieżek plików lub ścieżek z symbolami wieloznacznymi (* i ?). Gwiazdka reprezentuje zero lub więcej znaków. Znak zapytania reprezentuje jeden znak.

    Ważne

    Aby utworzyć kopię zapasową CDP folderu, trzeba wskazać jego zawartość za pomocą symbolu wieloznacznego gwiazdki:

    Poprawna ścieżka: `D:\Data\*`

    Niepoprawna ścieżka: `D:\Data\`

  - [W przypadku komputerów online] Aby bezpośrednio wybrać pliki i foldery:
    - W polu **Komputer używany do przeglądania** wybierz komputer, na którym znajdują się odpowiednie pliki lub foldery.
    - Kliknij **Wybierz pliki i foldery**, aby przeglądać foldery na wybranym komputerze.

      Bezpośrednio dokonany wybór powoduje utworzenie reguły wyboru. Jeśli plan ochrony zostanie zastosowany do wielu komputerów, a reguła wyboru nie ma zastosowania w przypadku danego komputera, zostanie pominięta na tym komputerze.

3. W panelu planu ochrony kliknij **Utwórz**.

Spowoduje to, że określone dane będą ciągle uwzględniane w kopii zapasowej między zaplanowanymi operacjami tworzenia kopii zapasowej.

Wybieranie miejsca docelowego

Kliknij **Miejsce docelowe kopii zapasowej** i wybierz jedną z następujących opcji:

- **Chmura**

  Kopie zapasowe będą przechowywane w chmurowym centrum danych.
- **Foldery lokalne**

  W przypadku wybrania jednego komputera przejdź do folderu na tym komputerze lub wpisz ścieżkę folderu.

  W przypadku wybrania wielu komputerów wpisz ścieżkę folderu. Kopie zapasowe będą przechowywane w tym folderze na każdym wybranym komputerze fizycznym lub na komputerze, na którym jest zainstalowany agent dla maszyn wirtualnych. Jeśli ten folder nie istnieje, zostanie utworzony.
- **Folder sieciowy**

  Jest to folder udostępniony za pośrednictwem udziału sieciowego SMB/CIFS/DFS.

© Acronis International GmbH, 2003-2024

Przejdź do wymaganego folderu udostępnionego lub wprowadź ścieżkę w następującym formacie:

- W przypadku udziałów SMB/CIFS: `\\<nazwa hosta>\<ścieżka>\` lub `smb://<nazwa hosta>/<ścieżka>/`
- W przypadku udziałów DFS: `\\<pełna nazwa domeny DNS>\<folder root DFS>\<ścieżka>`
  Na przykład: `\\przyklad.company.com\shared\files`

Następnie kliknij przycisk strzałki. Jeśli zostanie wyświetlony monit, określ nazwę użytkownika i hasło w celu uzyskania dostępu do folderu udostępnionego. Poświadczenia te można w każdej chwili zmienić, klikając ikonę klucza obok nazwy folderu.

Tworzenie kopii zapasowych w folderze z anonimowym dostępem nie jest obsługiwane.

- **Chmura publiczna**

  Ta opcja jest dostępna w ramach pakietu Zaawansowane tworzenie kopii zapasowych.

  Umożliwia ona skonfigurowanie operacji tworzenia kopii zapasowych bezpośrednio do pamięci masowej zgodnej z chmurą publiczną — bez konieczności wdrażania dodatkowych komponentów (takich jak platforma Microsoft Azure czy inne maszyny wirtualne jako bramy). Wybierz odpowiednią chmurę publiczną i ustanów z nią połączenie stosownie do potrzeb.

  Aby uzyskać więcej informacji, zobacz "Tworzenie kopii zapasowych obciążeń w chmurach publicznych" (s. 579).

- **Folder NFS** (dostępny na komputerach z systemem Linux lub macOS)

  Sprawdź, czy na serwerze Linux, na którym jest zainstalowany agent dla systemu Linux, jest też zainstalowany pakiet nfs-utils.

  Przejdź do wymaganego folderu NFS lub wprowadź ścieżkę w następującym formacie:

  `nfs://<nazwa hosta>/<wyeksportowany folder>:/<podfolder>`

  Następnie kliknij przycisk strzałki.

  Uwaga
  W folderze NFS chronionym hasłem nie można utworzyć kopii zapasowej.

- Strefa **Secure Zone** (dostępna, jeśli taka strefa znajduje się na każdym wybranym komputerze)

  Secure Zone to bezpieczna partycja na dysku komputera uwzględnianego w kopii zapasowej. Partycję tę trzeba utworzyć ręcznie przed skonfigurowaniem kopii zapasowej. Informacje na temat tworzenia partycji Secure Zone oraz jej zalet i wad można znaleźć w sekcji „"Secure Zone — informacje" (s. 443)”.

Zaawansowana opcja magazynu

Uwaga
Ta funkcja jest dostępna tylko w wersji Advanced usługi Cyber Protection.

Zdefiniowana za pomocą skryptu (dostępne w przypadku komputerów z systemem Windows)

Kopie zapasowej poszczególnych komputerów można przechowywać w folderze zdefiniowanym za pomocą skryptu. Oprogramowanie obsługuje skrypty napisane w języku JScript, VBScript lub Python

© Acronis International GmbH, 2003-2024

3.5. Wdrażając plan ochrony, oprogramowanie uruchamia skrypt na każdym komputerze. Wynikiem działania skryptu w przypadku każdego komputera powinna być ścieżka folderu lokalnego lub sieciowego. Jeśli folder nie istnieje, zostanie utworzony (ograniczenie: skrypty napisane w języku Python nie mogą tworzyć folderów w udziałach sieciowych). Na karcie **Magazyn kopii zapasowych** każdy folder jest pokazywany jako osobna lokalizacja kopii zapasowych.

W obszarze **Typ skryptu** wybierz typ skryptu (**JScript**, **VBScript** lub **Python**), a następnie zaimportuj lub skopiuj i wklej skrypt. W przypadku folderów sieciowych podaj poświadczenia dostępu z uprawnieniami do odczytu/zapisu.

Przykłady:

- Wynikiem działania poniższego skryptu JScript jest lokalizacja kopii zapasowych dla komputera w formacie `\\bkpsrv\<nazwa komputera>`:

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  W rezultacie kopie zapasowe poszczególnych komputerów będą zapisywane w folderze o tej samej nazwie na serwerze **bkpsrv**.
- Wynikiem działania poniższego skryptu JScript jest lokalizacja kopii zapasowych w folderze na komputerze, na którym działa skrypt:

  ```
  WScript.Echo("C:\\Backup");
  ```

  W związku z tym kopie zapasowe tego komputera będą zapisywane w folderze `C:\Backup` na tym samym komputerze.

  Uwaga
  Wielkość liter w ścieżce lokalizacji w tych skryptach ma znaczenie. Dlatego `C:\Backup` i `C:\backup` są widoczne w konsoli Cyber Protect jako różne lokalizacje. Ponadto jako litery dysku należy użyć wielkiej litery.

Secure Zone — informacje

Secure Zone to bezpieczna partycja na dysku komputera uwzględnianego w kopii zapasowej. Można na niej przechowywać kopie zapasowe dysków lub plików danego komputera.

W przypadku fizycznej usterki dysku można stracić kopie zapasowe ze strefy Secure Zone. Dlatego strefa Secure Zone nie powinna być jedyną lokalizacją do przechowywania kopii zapasowych. W infrastrukturze przedsiębiorstwa strefa Secure Zone może służyć jako pośrednia lokalizacja kopii zapasowych, używana w przypadku, gdy normalna lokalizacja jest tymczasowo niedostępna albo podłączona poprzez powolny lub obciążony kanał przesyłowy.

Dlaczego warto korzystać ze strefy Secure Zone?

Secure Zone:

© Acronis International GmbH, 2003-2024

- Umożliwia odzyskanie zawartości dysku na ten sam dysk, na którym znajduje się jego kopia zapasowa.
- Stanowi oszczędną i wygodną metodę ochrony danych przed usterkami oprogramowania, atakami wirusów i błędami użytkowników.
- Eliminuje konieczność użycia dodatkowego nośnika lub połączenia sieciowego w celu utworzenia kopii zapasowej bądź odzyskania danych. Szczególnie przydaje się to użytkownikom mobilnym.
- Może służyć jako podstawowe miejsce docelowe w przypadku korzystania z replikacji kopii zapasowych.

Ograniczenia

- strefy Secure Zone nie można utworzyć na komputerze Mac.
- Secure Zone jest partycją lokalizowaną na dysku standardowym. Nie można jej utworzyć na dysku dynamicznym ani utworzyć jako wolumin logiczny (zarządzany przy użyciu menedżera LVM).
- Secure Zone jest formatowana w systemie plików FAT32. Ponieważ w systemie FAT32 rozmiar plików jest ograniczony do 4 GB, większe kopie zapasowe są dzielone podczas zapisywania w strefie Secure Zone. Nie ma to wpływu na procedurę ani szybkość odzyskiwania.

Jak utworzenie strefy Secure Zone wpływa na dysk

- Strefa Secure Zone jest zawsze tworzona na końcu dysku twardego.
- Jeśli na końcu dysku nie ma wystarczającej ilości nieprzydzielonego miejsca, ale istnieje ono między woluminami, woluminy są przenoszone w celu zwiększenia ilości nieprzydzielonego miejsca na końcu dysku.
- Jeśli mimo zgromadzenia całego nieprzydzielonego miejsca jego ilość jest wciąż niewystarczająca, oprogramowanie zajmuje wolne miejsce na wybranych woluminach, zmniejszając proporcjonalnie ich rozmiar.
- Na woluminie powinno jednak pozostać wolne miejsce, wymagane do prawidłowego działania systemu operacyjnego i aplikacji (na przykład do tworzenia plików tymczasowych). Oprogramowanie nie zmniejszy rozmiaru woluminu, na którym ilość wolnego miejsca jest lub stałaby się mniejsza niż 25 procent rozmiaru woluminu. Proporcjonalne zmniejszanie rozmiaru woluminów będzie kontynuowane tylko wtedy, gdy wszystkie woluminy na dysku będą zawierać 25 procent lub mniej wolnego miejsca.

Jak widać powyżej, lepiej nie ustawiać maksymalnego rozmiaru strefy Secure Zone. W efekcie na żadnym woluminie nie pozostanie wolne miejsce, wskutek czego system operacyjny lub aplikacje mogą działać niestabilnie lub w ogóle się nie uruchamiać.

Ważne
Przeniesienie lub zmiana rozmiaru woluminu, z którego jest uruchamiany system, wymaga ponownego uruchomienia komputera.

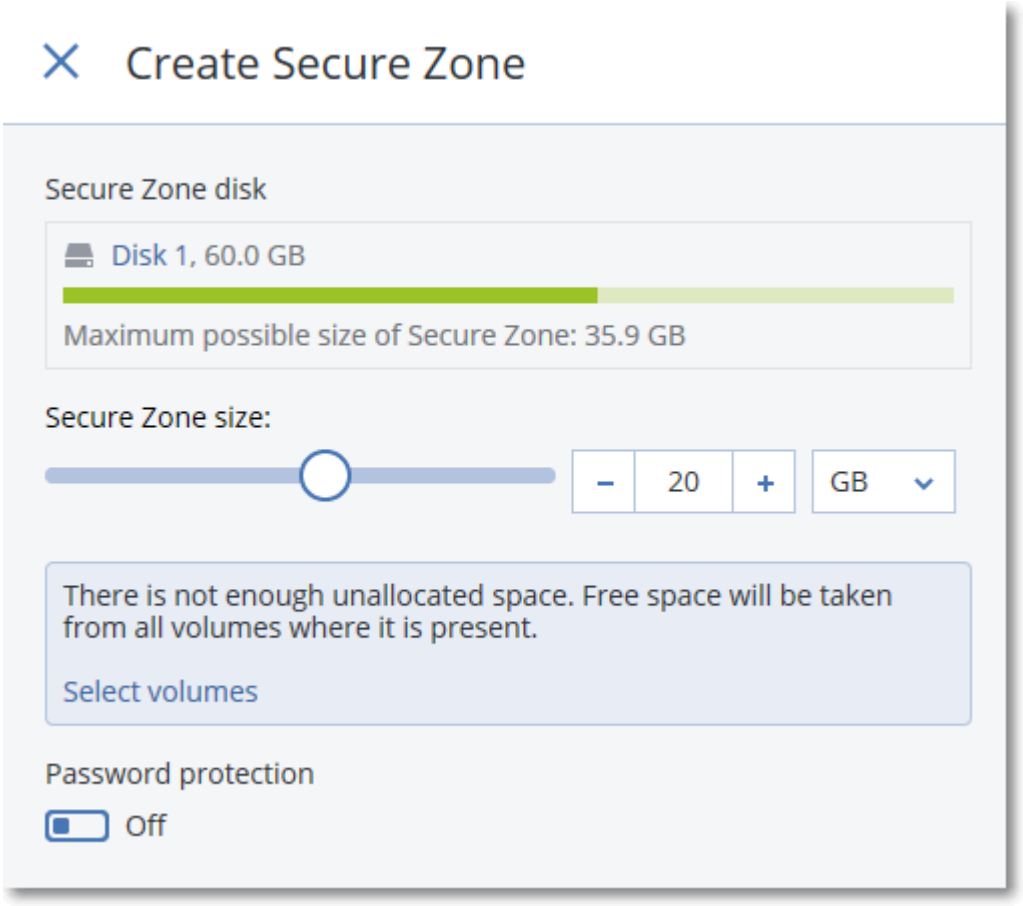
© Acronis International GmbH, 2003-2024

Jak utworzyć strefę Secure Zone

1. Wybierz komputer, na którym chcesz utworzyć strefę Secure Zone.
2. Kliknij **Szczegóły** > **Utwórz strefę Secure Zone**.
3. W obszarze **Dysk strefy Secure Zone** kliknij **Wybierz**, a następnie wybierz dysk twardy (jeśli jest ich kilka), na którym ma zostać utworzona strefa.

   Oprogramowanie obliczy maksymalny rozmiar strefy Secure Zone.
4. Wprowadź rozmiar strefy Secure Zone lub przeciągnij suwak w celu wybrania dowolnego rozmiaru między wartościami minimalną i maksymalną.

   Minimalny rozmiar to około 50 MB, w zależności od geometrii dysku twardego. Rozmiar maksymalny jest równy sumie ilości nieprzydzielonego miejsca na dysku oraz łącznej ilości wolnego miejsca na wszystkich woluminach dysku.
5. Jeśli nieprzydzielonego miejsca jest zbyt mało na określony rozmiar, oprogramowanie zajmie wolne miejsce z istniejących woluminów. Domyślnie wybrane są wszystkie woluminy. Jeśli chcesz wykluczyć jakieś woluminy, kliknij **Wybierz woluminy**. W przeciwnym razie pomiń ten krok.



6. [Opcjonalnie] Włącz przełącznik **Ochrona hasłem** i określ hasło.

   Hasło to będzie wymagane podczas uzyskiwania dostępu do kopii zapasowych znajdujących się w strefie Secure Zone. Utworzenie kopii zapasowej w strefie Secure Zone nie wymaga hasła, chyba że kopia jest tworzona przy użyciu nośnika startego.

© Acronis International GmbH, 2003-2024

7. Kliknij **Utwórz**.

   Oprogramowanie wyświetli spodziewany układ partycji. Kliknij **OK**.
8. Poczekaj, aż oprogramowanie utworzy strefę Secure Zone.

Teraz podczas tworzenia planu ochrony możesz w sekcji **Miejsce docelowe kopii zapasowej** wybrać strefę Secure Zone.

Jak usunąć strefę Secure Zone

1. Wybierz komputer ze strefą Secure Zone.
2. Kliknij opcję **Szczegóły**.
3. Kliknij ikonę koła zębatego widoczną obok strefy **Secure Zone**, a następnie kliknij **Usuń**.
4. [Opcjonalnie] Określ woluminy, do których zostanie dodane miejsce zwolnione przez strefę. Domyślnie wybrane są wszystkie woluminy.

   Miejsce zostanie równo rozdzielone między wybrane woluminy. W przypadku niewybrania żadnego woluminu zwolnione miejsce będzie nieprzydzielone.

   Zmiana rozmiaru woluminu, z którego uruchamiany jest system, wymaga ponownego uruchomienia komputera.
5. Kliknij **Usuń**.

W wyniku tego strefa Secure Zone zostanie usunięta wraz ze wszystkimi przechowywanymi w niej kopiami zapasowymi.

Harmonogram tworzenia kopii zapasowych

Operacje tworzenia kopii zapasowych można skonfigurować tak, aby były uruchamiane automatycznie o określonej godzinie, w określonych odstępach czasu lub po wystąpieniu określonego zdarzenia.

Zaplanowane operacje tworzenia kopii zapasowych zasobów innych niż międzychmurowe są wykonywane według ustawień strefy czasowej obciążenia, na którym jest zainstalowany agent ochrony. Jeśli na przykład ten sam plan ochrony zostanie zastosowany do obciążeń z różnymi ustawieniami stref czasowych, operacje tworzenia kopii zapasowych będą uruchamiane zgodnie z lokalną strefą czasową poszczególnych obciążeń.

Planowanie operacji tworzenia kopii zapasowej obejmuje następujące czynności:

- Wybranie schematu tworzenia kopii zapasowych
- Skonfigurowanie czasu lub wybranie zdarzenia wyzwalającego operację tworzenia kopii zapasowej
- Skonfigurowanie ustawień opcjonalnych i warunków rozpoczęcia

© Acronis International GmbH, 2003-2024

Schematy tworzenia kopii zapasowych

Schemat tworzenia kopii zapasowych stanowi tę część harmonogramu planu ochrony, która definiuje, jakiego typu kopia zapasowa (pełna, różnicowa czy przyrostowa) jest tworzona i kiedy. Możesz wybrać jeden z gotowych schematów tworzenia kopii zapasowych lub utworzyć schemat niestandardowy.

Dostępne schematy tworzenia i typy kopii zapasowych zależą od lokalizacji i źródła kopii zapasowych. Na przykład różnicowa kopia zapasowa nie jest dostępna w przypadku tworzenia kopii zapasowych danych SQL, danych programu Exchange lub stanu systemu. Schemat **Zawsze przyrostowa (jednoplikowa)** nie jest obsługiwany w przypadku urządzeń taśmowych.

Schemat tworzenia kopii zapasowych	Opis	Konfigurowalne elementy
Zawsze przyrostowa (jednoplikowa)	Pierwsza kopia zapasowa jest pełna i jej utworzenie może być czasochłonne. Kolejne kopie zapasowe są przyrostowe i ich utworzenie zajmuje znacznie mniej czasu. W przypadku tych kopii zapasowych będzie stosowany format jednoplikowych kopii zapasowych[1]*. Domyślnie kopie zapasowe są tworzone codziennie od poniedziałku do piątku. Zalecamy korzystanie z tego schematu w przypadku zapisywania kopii zapasowych w chmurze, ponieważ przyrostowe kopie zapasowe są tworzone szybko i wiążą się ze znacznie mniejszym ruchem sieciowym.	• Typ harmonogramu: co miesiąc, co tydzień, codziennie, co godzinę • Wyzwalacz operacji tworzenia kopii zapasowej: czas lub zdarzenie • Godzina rozpoczęcia • Warunki rozpoczęcia • Opcje dodatkowe
Zawsze pełne	Wszystkie kopie zapasowe w zestawie są pełne. Domyślnie kopie zapasowe są tworzone codziennie od poniedziałku do piątku.	• Typ harmonogramu: co miesiąc, co tydzień, codziennie, co godzinę • Wyzwalacz operacji tworzenia kopii zapasowej: czas lub zdarzenie

[1]Format kopii zapasowych, w którym początkowa pełna kopia zapasowa i późniejsze przyrostowe kopie zapasowe są zapisywane w jednym pliku .tibx. W formacie tym wykorzystano szybkość metody tworzenia przyrostowych kopii zapasowych, unikając najpoważniejszej wady tej metody — trudności związanych z usuwaniem przestarzałych kopii zapasowych. Oprogramowanie oznacza bloki zajmowane przez przestarzałe kopie zapasowe jako „wolne" i korzysta z nich podczas zapisywania nowych kopii zapasowych. Umożliwia to nadzwyczaj szybkie czyszczenie przy minimalnym obciążeniu zasobów. Ten format jednoplikowej kopii zapasowej nie jest dostępny w przypadku tworzenia kopii zapasowej w lokalizacji nieobsługujących odczytu i zapisu z dostępem losowym.

© Acronis International GmbH, 2003-2024

Schemat tworzenia kopii zapasowych	Opis	Konfigurowalne elementy
		• Godzina rozpoczęcia • Warunki rozpoczęcia • Opcje dodatkowe
Tygodniowe pełne, dzienne przyrostowe	Pełna kopia zapasowa jest tworzona raz w tygodniu, a pozostałe kopie zapasowe są przyrostowe. Pierwsza kopia zapasowa jest pełna, a pozostałe kopie zapasowe w ciągu tygodnia są przyrostowe, po czym cykl się powtarza. Aby wybrać dzień tworzenia tygodniowej pełnej kopii zapasowej, w planie ochrony kliknij ikonę koła zębatego, a następnie wybierz kolejno **Opcje tworzenia kopii zapasowych** > **Tygodniowa kopia zapasowa**. Domyślnie kopie zapasowe są tworzone codziennie od poniedziałku do piątku.	• Wyzwalacz operacji tworzenia kopii zapasowej: czas lub zdarzenie • Godzina rozpoczęcia • Warunki rozpoczęcia • Opcje dodatkowe
Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe (GFS)	Domyślnie przyrostowe kopie zapasowe są tworzone codziennie od poniedziałku do piątku. Różnicowe kopie zapasowe są tworzone w każdą sobotę. Pełne kopie zapasowe są tworzone pierwszego dnia każdego miesiąca. **Uwaga** Jest to gotowy specjalny schemat. W planie ochrony jest on oznaczony jako **Niestandardowy**.	• Zmień istniejący już harmonogram z uwzględnieniem typu kopii zapasowej: ◦ Typ harmonogramu: co miesiąc, co tydzień, codziennie, co godzinę ◦ Wyzwalacz operacji tworzenia kopii zapasowej: czas lub zdarzenie ◦ Godzina rozpoczęcia ◦ Warunki rozpoczęcia ◦ Opcje dodatkowe • Dodaj nowe harmonogramy z uwzględnieniem typu kopii zapasowej
Niestandardowe	Należy wybrać typy kopii zapasowych (pełne,	• Zmień istniejący już

© Acronis International GmbH, 2003-2024

Schemat tworzenia kopii zapasowych	Opis	Konfigurowalne elementy
	różnicowe i przyrostowe) oraz skonfigurować osobny harmonogram dla każdego z nich*.	harmonogram z uwzględnieniem typu kopii zapasowej: ◦ Typ harmonogramu: co miesiąc, co tydzień, codziennie, co godzinę ◦ Wyzwalacz operacji tworzenia kopii zapasowej: czas lub zdarzenie ◦ Godzina rozpoczęcia ◦ Warunki rozpoczęcia ◦ Opcje dodatkowe • Dodaj nowe harmonogramy z uwzględnieniem typu kopii zapasowej

* Po utworzeniu planu ochrony nie można przełączać między schematem tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** a innymi schematami tworzenia kopii zapasowych. **Zawsze przyrostowa (jednoplikowa)** to schemat oparty na formacie jednoplikowym, a pozostałe schematy są oparte na formacie wieloplikowym. Aby przełączać formaty, utwórz nowy plan ochrony.

Typy kopii zapasowych

Dostępne są następujące typy kopii zapasowych:

- Pełna — pełna kopia zapasowa zawiera wszystkie dane źródłowe. Jest to kopia samowystarczalna. Nie trzeba mieć dostępu do żadnych innych kopii zapasowych, aby odzyskać dane.

  Uwaga
  Pierwsza kopia zapasowa tworzona w ramach dowolnego planu ochrony jest zawsze pełną kopią zapasową.

- Przyrostowa — w przyrostowej kopii zapasowej są przechowywane dane, które uległy zmianie od czasu utworzenia ostatniej kopii zapasowej, niezależnie od tego, czy była to pełna, różnicowa czy przyrostowa kopia zapasowa. Do odzyskania danych potrzebny jest cały łańcuch kopii zapasowych, od których zależy przyrostowa kopia zapasowa — aż do pierwszej pełnej kopii

© Acronis International GmbH, 2003-2024

zapasowej.

- Różnicowa — w różnicowej kopii zapasowej są przechowywane dane, które uległy zmianie od czasu utworzenia ostatniej pełnej kopii zapasowej. Do odzyskania danych potrzebna jest zarówno różnicowa kopia zapasowa, jak i pełna kopia zapasowa, od której zależy kopia różnicowa.

Uruchamianie operacji tworzenia kopii zapasowej zgodnie z harmonogramem

Aby operacja tworzenia kopii zapasowej została automatycznie uruchomiona o określonej godzinie lub w przypadku określonego zdarzenia, włącz harmonogram w planie ochrony.

Aby włączyć harmonogram

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. Kliknij **Harmonogram**.
3. Włącz przełącznik harmonogramu.
4. Wybierz schemat tworzenia kopii zapasowych.
5. Skonfiguruj harmonogram stosownie do potrzeb i kliknij **Gotowe**.
   Dodatkowe informacje na temat dostępnych opcji planowania można znaleźć w sekcjach "Zaplanuj według czasu" (s. 450) i "Harmonogram jest oparty na zdarzeniach." (s. 453).
6. [Opcjonalnie] Skonfiguruj warunki rozpoczęcia lub dodatkowe opcje planowania.
7. Zapisz plan ochrony.

W wyniku tych działań operacja tworzenia kopii zapasowej rozpocznie się za każdym razem, gdy zostaną spełnione warunki harmonogramu.

Aby wyłączyć harmonogram

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. Kliknij **Harmonogram**.
3. Wyłącz przełącznik harmonogramu.
4. Zapisz plan ochrony.

W wyniku tych działań operacja tworzenia kopii zapasowej rozpocznie się tylko wtedy, gdy ją uruchomisz ręcznie.

Uwaga
W przypadku wyłączenia harmonogramu reguły przechowywania nie będą stosowane automatycznie. Aby je zastosować, należy ręcznie uruchomić operację tworzenia kopii zapasowej.

Zaplanuj według czasu

W poniższej tabeli zestawiono opcje planowania dotyczące czasu. Dostępność tych opcji zależy schematu tworzenia kopii zapasowych. Aby uzyskać więcej informacji, zobacz "Schematy tworzenia

© Acronis International GmbH, 2003-2024

kopii zapasowych" (s. 447).

Opcja	Opis	Przykłady
Co miesiąc	Wybierz miesiące, dni miesiąca lub dni tygodnia, a następnie godzinę rozpoczęcia tworzenia kopii zapasowej.	Uruchom operację tworzenia kopii zapasowej 1 stycznia i 3 lutego o 00:00. Uruchom operację tworzenia kopii zapasowej pierwszego dnia każdego miesiąca o 10:00. Uruchom operację tworzenia kopii zapasowej 1 marca, 5 marca, 1 kwietnia i 5 kwietnia o 09:00. Uruchom operację tworzenia kopii zapasowej w drugi i trzeci piątek każdego miesiąca o 11:00. Uruchom operację tworzenia kopii zapasowej w ostatnią środę miesiąca o 22:30.
Co tydzień	Wybierz dni tygodnia, a następnie godzinę rozpoczęcia operacji tworzenia kopii zapasowej.	Uruchamiaj operację tworzenia kopii zapasowej od poniedziałku do piątku o 10:00. Uruchamiaj operację tworzenia kopii zapasowej w poniedziałek o 23:00. Uruchamiaj operację tworzenia kopii zapasowej we wtorek i sobotę o 08:00.
Codziennie	Wybierz dni (dowolne lub tylko robocze), a następnie godzinę rozpoczęcia operacji tworzenia kopii zapasowej.	Uruchamiaj operację tworzenia kopii zapasowej codziennie o 11:45. Uruchamiaj operację tworzenia kopii zapasowej od poniedziałku do piątku o 21:30.
Co godzinę	Wybierz dni tygodnia, a następnie odstęp czasowy między dwiema kolejnymi operacjami tworzenia kopii zapasowych i zakres czasu, w którym takie operacje będą uruchamiane. Konfigurując odstęp w minutach, możesz wybrać proponowany odstęp wynoszący od 10 do 60 minut lub podać niestandardowy odstęp, na przykład 45 lub 75 minut.	Uruchamiaj operację tworzenia kopii zapasowej od poniedziałku do piątku między 08:00 a 18:00. Uruchamiaj operację tworzenia kopii zapasowej co 3 godziny w sobotę i niedzielę między 01:00 a 18:00.

© Acronis International GmbH, 2003-2024

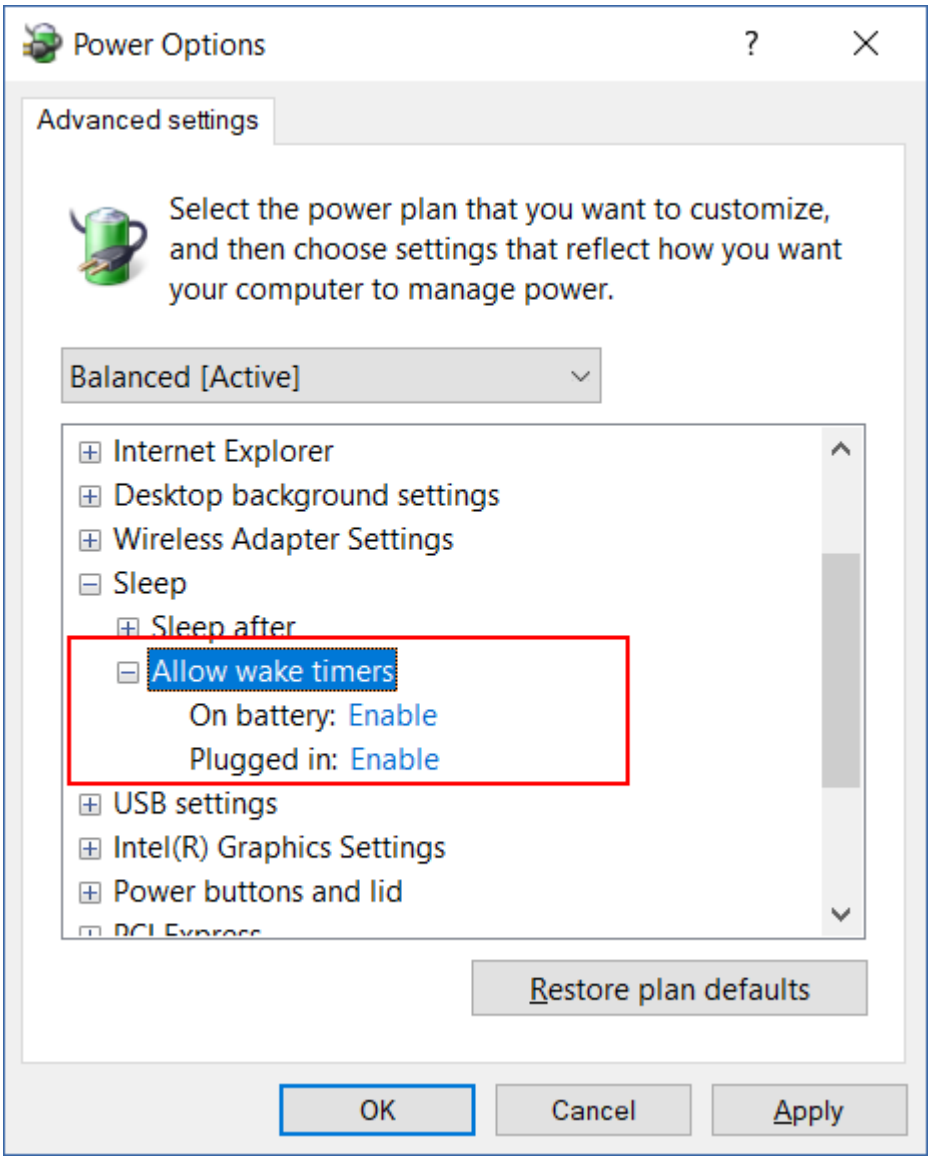
Opcje dodatkowe

W przypadku planowania tworzenia kopii zapasowej według czasu dostępne są następujące dodatkowe opcje planowania.

Aby uzyskać do nich dostęp, w okienku **Harmonogram** kliknij **Pokaż więcej**.

- **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu**
  Ustawienie domyślne: Wyłączono.
- **Zapobiegaj włączaniu trybu uśpienia lub hibernacji podczas tworzenia kopii zapasowych**
  Ta opcja ma zastosowanie tylko komputerów z systemem Windows.
  Ustawienie domyślne: Włączono.
- **Wznów pracę z trybu uśpienia lub hibernacji, aby rozpocząć planowaną operację tworzenia kopii zapasowej**
  Ta opcja ma zastosowanie tylko do komputerów z systemem Windows w planach zasilania, w których przypadku włączono opcję **Zezwalaj na wznawianie pracy według czasomierza**.

© Acronis International GmbH, 2003-2024



Ta opcja nie korzysta z funkcji Wake-on-LAN i nie ma zastosowania do wyłączonych komputerów.

Ustawienie domyślne: Wyłączono.

Harmonogram jest oparty na zdarzeniach.

Aby skonfigurować operację tworzenia kopii zapasowej uruchamianą po wystąpieniu określonego zdarzenia, wybierz jedną z poniższych opcji.

Opcja	Opis	Przykłady
Po upływie określonego czasu od utworzenia ostatniej kopii zapasowej	Operacja tworzenia kopii zapasowej jest uruchamiana po upływie określonego czasu od ostatniej pomyślnej operacji tworzenia kopii zapasowej.	Uruchom operację tworzenia kopii zapasowej dzień po ostatniej pomyślnie wykonanej operacji tworzenia kopii zapasowej. Uruchom operację tworzenia kopii zapasowej cztery godziny po ostatniej

© Acronis International GmbH, 2003-2024

Opcja	Opis	Przykłady
	Uwaga Ta opcja zależy od tego, jak zakończyła się poprzednia operacja tworzenia kopii zapasowej. Jeśli utworzenie kopii zapasowej się nie powiedzie, następna operacja tworzenia kopii zapasowej nie zostanie rozpoczęta automatycznie. W takim przypadku należy ręcznie uruchomić operację tworzenia kopii zapasowej i upewnić się, że zakończyła się ona pomyślnie, aby zresetować harmonogram.	pomyślnie wykonanej operacji tworzenia kopii zapasowej.
Gdy użytkownik zaloguje się w systemie	Operacja tworzenia kopii zapasowej jest uruchamiana, gdy użytkownik zaloguje się na komputerze. Opcję tę można skonfigurować z uwzględnieniem każdego zalogowania się lub zalogowania się określonego użytkownika. **Uwaga** Zalogowanie się przy użyciu tymczasowego profilu użytkownika nie spowoduje uruchomienia operacji tworzenia kopii zapasowej.	Uruchom operację tworzenia kopii zapasowej po zalogowaniu się użytkownika Jan Kowalski.
Gdy użytkownik wyloguje się z systemu	Operacja tworzenia kopii zapasowej jest uruchamiana, gdy użytkownik wyloguje się z komputera. Opcję tę można skonfigurować z uwzględnieniem każdego wylogowania się lub wylogowania się określonego użytkownika. **Uwaga** Wylogowanie się z tymczasowego profilu użytkownika nie spowoduje uruchomienia operacji tworzenia kopii zapasowej. Zamykanie systemu komputera lub maszyny nie spowoduje uruchomienia operacji tworzenia kopii zapasowej.	Uruchom tworzenie kopii zapasowej po wylogowaniu się wszystkich użytkowników.
Podczas	Operacja tworzenia kopii zapasowej	Uruchom tworzenie kopii zapasowej po

© Acronis International GmbH, 2003-2024

Opcja	Opis	Przykłady
uruchamiania systemu	zostanie uruchomiona po uruchomieniu chronionego komputera.	uruchomieniu komputera przez użytkownika.
Podczas zamknięcia systemu	Operacja tworzenia kopii zapasowej zostanie uruchomiona po wyłączeniu chronionego komputera.	Uruchom tworzenie kopii zapasowej po wyłączeniu komputera przez użytkownika.
Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows	Operacja tworzenia kopii zapasowej zostanie uruchomiona po wystąpieniu określonego zdarzenia systemu Windows.	Uruchom tworzenie kopii zapasowej, gdy zdarzenie 7 typu błąd i źródło dysk zostaną zarejestrowanie w dzienniku systemu Windows.

Dostępność tych opcji zależy od źródła kopii zapasowej i systemu operacyjnego chronionego obciążenia. Poniższa tabela zawiera zestawienie dostępnych opcji w przypadku systemów Windows, Linux i macOS.

Zdarzenie	Źródło kopii zapasowej (Elementy uwzględniane w kopii zapasowej)					
	Cały komputer, Dyski/woluminy lub Pliki/foldery (komputery fizyczne)	**Cały komputer lub Dyski/woluminy (maszyny wirtualne)**	**Konfiguracja ESXi**	**Skrzynki pocztowe Microsoft 365**	**Bazy danych i skrzynki pocztowe programu Exchange**	**Bazy danych SQL**
Po upływie określonego czasu od utworzenia ostatniej kopii zapasowej	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Gdy użytkownik zaloguje się w systemie	Windows	N.d.	N.d.	N.d.	N.d.	N.d.
Gdy użytkownik wyloguje się z systemu	Windows	N.d.	N.d.	N.d.	N.d.	N.d.
Podczas uruchamiania systemu	Windows, Linux, macOS	N.d.	N.d.	N.d.	N.d.	N.d.

© Acronis International GmbH, 2003-2024

Zdarzenie	Źródło kopii zapasowej (Elementy uwzględniane w kopii zapasowej)					
	Cały komputer, Dyski/woluminy lub Pliki/foldery (komputery fizyczne)	**Cały komputer lub Dyski/woluminy (maszyny wirtualne)**	**Konfiguracja ESXi**	**Skrzynki pocztowe Microsoft 365**	**Bazy danych i skrzynki pocztowe programu Exchange**	**Bazy danych SQL**
Podczas zamknięcia systemu	Windows	N.d.	N.d.	N.d.	N.d.	N.d.
Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows	Windows	N.d.	N.d.	Windows	Windows	Windows

Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows

Operacja tworzenia kopii zapasowej może zostać uruchomiona automatycznie po zarejestrowaniu określonego zdarzenia w dzienniku zdarzeń systemu Windows, takim jak dziennik aplikacji, dziennik zabezpieczeń czy dziennik systemowy.

Uwaga
Zdarzenia i ich właściwości można przeglądać w sekcji **Zarządzanie komputerem** > **Podgląd zdarzeń** w systemie Windows. Aby otworzyć dziennik zabezpieczeń, trzeba mieć uprawnienia administratora.

Parametry zdarzenia

W poniższej tabeli zestawiono parametry, które należy dodać w przypadku konfigurowania opcji **Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows**.

Parametr	Opis
Nazwa dziennika	Nazwa dziennika. Wybierz nazwę dziennika standardowego (Aplikacja, Zabezpieczenia lub System) lub podaj nazwę innego dziennika. Na przykład Sesje Microsoft Office.
Źródło zdarzenia	Źródło zdarzenia oznacza program lub komponent systemu, który spowodował zdarzenie. Na przykład dysk.

© Acronis International GmbH, 2003-2024

Parametr	Opis
	Źródło zdarzenia, które zawiera określony ciąg znaków, spowoduje uruchomienie zaplanowanej operacji tworzenia kopii zapasowej. W przypadku tej opcji nie jest rozróżniana wielkość liter. W przypadku podania ciągu znaków `service` operację tworzenia kopii zapasowej wywoła zarówno źródło zdarzeń Menedżer kontroli usługi, jak i Usługa czasu.
Typ zdarzenia	Typ zdarzenia: Błąd, Ostrzeżenie, Informacja, Powodzenie inspekcji lub Niepowodzenie inspekcji.
Identyfikator zdarzenia	Identyfikator zdarzenia identyfikuje określony rodzaj zdarzenia w źródle zdarzeń. Na przykład zdarzenie Błąd o źródle dysk i identyfikatorze 7 występuje wtedy, gdy system Windows wykryje na dysku uszkodzony sektor, natomiast zdarzenie Błąd o źródle dysk i identyfikatorze 15 występuje wtedy, gdy dysk nie jest gotowy, by można było uzyskać do niego dostęp.

Przykład: Awaryjna kopia zapasowa po wykryciu uszkodzonych sektorów na dysku twardym

Nawet jeden uszkodzony sektor na dysku twardym może sygnalizować bliską awarię. Dlatego po wykryciu nieprawidłowego sektora warto utworzyć kopię zapasową.

Gdy system Windows wykryje uszkodzony sektor na dysku, w dzienniku systemowym zostanie zarejestrowane zdarzenie błędu z numerem 7 i źródłem zdarzenia dysk. W planie ochrony skonfiguruj następujący harmonogram:

- Harmonogram: Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows
- Nazwa dziennika: System
- Źródło zdarzenia: disk
- Typ zdarzenia: Błąd
- Identyfikator zdarzenia: 7

Ważne
Aby się upewnić, że operacja tworzenia kopii zapasowej zostanie ukończona mimo uszkodzonych sektorów, w sekcji **Opcje tworzenia kopii zapasowej** przejdź do pozycji **Obsługa błędów**, a następnie zaznacz pole wyboru **Ignoruj uszkodzone sektory**.

Warunki rozpoczęcia

Aby operacja tworzenia kopii zapasowej była uruchamiana tylko wtedy, gdy są spełnione określone warunki, należy skonfigurować co najmniej jeden warunek rozpoczęcia. W przypadku skonfigurowania wielu warunków operacja tworzenia kopii zapasowej zostanie uruchomiona dopiero wtedy, gdy wszystkie te warunki zostaną spełnione. Można określić okres, po którym

© Acronis International GmbH, 2003-2024

operacje tworzenia kopii zapasowych będą uruchamiane bez względu na to, czy warunki zostały spełnione. Dodatkowe informacje na temat tej opcji tworzenia kopii zapasowych można znaleźć w sekcji "Warunki uruchomienia zadania" (s. 526).

Warunków rozpoczęcia nie da się zastosować w przypadku ręcznego uruchamiania operacji tworzenia kopii zapasowej.

W poniższej tabeli wymieniono warunki uruchomienia zadania dostępne w przypadku różnych danych w systemach Windows, Linux i macOS.

Warunek rozpoczęcia	**Źródło kopii zapasowej (Elementy uwzględniane w kopii zapasowej)**					
	Cały komputer, Dyski/woluminy lub Pliki/foldery (komputery fizyczne)	**Cały komputer lub Dyski/woluminy (maszyny wirtualne)**	**Konfiguracja ESXi**	**Skrzynki pocztowe Microsoft 365**	**Bazy danych i skrzynki pocztowe programu Exchange**	**Bazy danych SQL**
Użytkownik jest bezczynny	Windows	N.d.	N.d.	N.d.	N.d.	N.d.
Host lokalizacji kopii zapasowej jest dostępny	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Użytkownicy są wylogowani	Windows	N.d.	N.d.	N.d.	N.d.	N.d.
Mieści się w przedziale czasu	Windows, Linux, macOS	Windows, Linux	N.d.	N.d.	N.d.	N.d.
Oszczędzaj baterię	Windows	N.d.	N.d.	N.d.	N.d.	N.d.
Nie uruchamiaj przy połączeniu taryfowym	Windows	N.d.	N.d.	N.d.	N.d.	N.d.
Nie uruchamiaj przy	Windows	N.d.	N.d.	N.d.	N.d.	N.d.

© Acronis International GmbH, 2003-2024

Warunek rozpoczęcia	Źródło kopii zapasowej (Elementy uwzględniane w kopii zapasowej)					
	Cały komputer, Dyski/woluminy lub Pliki/foldery (komputery fizyczne)	**Cały komputer lub Dyski/woluminy (maszyny wirtualne)**	**Konfiguracja ESXi**	**Skrzynki pocztowe Microsoft 365**	**Bazy danych i skrzynki pocztowe programu Exchange**	**Bazy danych SQL**
połączeniu z następującym i sieciami Wi-Fi						
Sprawdź adres IP urządzenia	Windows	N.d.	N.d.	N.d.	N.d.	N.d.

Użytkownik jest bezczynny

„Użytkownik jest bezczynny" oznacza, że na komputerze jest uruchomiony wygaszacz ekranu lub komputer jest zablokowany.

Przykład

Uruchamiaj operację tworzenia kopii zapasowej codziennie o 21:00, najlepiej w czasie bezczynności użytkownika. Jeśli o 23:00 użytkownik wciąż jest aktywny, kopia zapasowa ostanie utworzona mimo to.

- Harmonogram: **Codziennie**, **Uruchamiaj codziennie**. Uruchom o: **21:00**.
- Warunek: **Użytkownik jest bezczynny**.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Poczekaj na spełnienie warunków**, **Rozpocznij zadanie mimo wszystko po 2** godz.

Wskutek tego:

- Jeśli użytkownik przejdzie w stan bezczynności przed 21:00, tworzenie kopii zapasowej rozpocznie się o 21:00.
- Jeśli użytkownik przejdzie w stan bezczynności między 21:00 a 23:00, tworzenie kopii zapasowej rozpocznie się od razu.
- Jeśli o godzinie 23:00 użytkownik nadal będzie aktywny, tworzenie kopii zapasowej rozpocznie się o godzinie 23:00.

Host lokalizacji kopii zapasowej jest dostępny

Komunikat „Host lokalizacji kopii zapasowej jest dostępny" oznacza, że komputer służący jako host lokalizacji kopii zapasowej jest dostępny za pośrednictwem sieci.

© Acronis International GmbH, 2003-2024

Ten warunek ma zastosowanie do folderów sieciowych, chmury i lokalizacji zarządzanych przez węzeł magazynowania.

Ten warunek nie dotyczy dostępności samej lokalizacji, a jedynie dostępności hosta. Jeśli na przykład host jest dostępny, ale folder sieciowy na tym hoście nie jest udostępniony lub poświadczenia folderu nie są już ważne, ten warunek nadal jest uznawany za spełniony.

Przykład

W każdy dzień roboczy o 21:00 jest tworzona kopia zapasowa w folderze sieciowym. Jeśli komputer będący hostem folderu nie jest dostępny w danej chwili (na przykład z powodu konserwacji), należy pominąć tworzenie kopii zapasowej i zaczekać na planowane rozpoczęcie następnego dnia roboczego.

- Harmonogram: **Codziennie**, **Uruchamiaj od poniedziałku do piątku**. Uruchom o: **21:00**.
- Warunek: **Host lokalizacji kopii zapasowej jest dostępny.**
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Pomiń zaplanowaną operację tworzenia kopii zapasowej.**

Wskutek tego:

- Jeśli host jest dostępny o 21:00, operacja tworzenia kopii zapasowych rozpocznie się od razu.
- Jeśli host nie jest dostępny o 21:00, operacja tworzenia kopii zapasowych rozpocznie się w następny dzień roboczy (jeśli host będzie dostępny o godzinie 21:00 w tym dniu).
- Jeśli host nigdy nie jest dostępny o 21:00 w dni robocze, tworzenie kopii zapasowej w ogóle się nie rozpocznie.

Użytkownicy są wylogowani

Ten warunek rozpoczęcia umożliwia odłożenie operacji tworzenia kopii zapasowej do momentu wylogowania się wszystkich użytkowników z komputera z systemem Windows.

Przykład

Tworzenie kopii zapasowej rozpoczyna się w każdy piątek o 20:00, najlepiej wtedy, gdy wszyscy użytkownicy są wylogowani. Jeśli o 23:00 jeden z użytkowników wciąż jest zalogowany, tworzenie kopii zapasowej rozpocznie się mimo to.

- Harmonogram: **Co tydzień**, w piątki. Uruchom o: **20:00**.
- Warunek: **Użytkownicy są wylogowani**.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Poczekaj na spełnienie warunków**, **Mimo to rozpocznij tworzenie kopii zapasowej po 3** godz.

Wskutek tego:

- Jeśli o 20:00 wszyscy użytkownicy będą wylogowani, tworzenie kopii zapasowej rozpocznie się o 20:00.

© Acronis International GmbH, 2003-2024

- Jeśli ostatni użytkownik wyloguje się między 20:00 a 23:00, tworzenie kopii zapasowej rozpocznie się od razu.
- Jeśli o 23:00 nadal będą zalogowani jacyś użytkownicy, tworzenie kopii zapasowej rozpocznie się o godzinie 23:00.

Zadanie mieści się w przedziale czasu

Użyj tego warunku rozpoczęcia w celu ograniczenia uruchomienia operacji tworzenia kopii zapasowej do określonego przedziału czasu.

Przykład

Firma tworzy kopie zapasowe danych użytkowników i serwerów w różnych miejscach w tej samej sieciowej pamięci masowej.

Dzień roboczy rozpoczyna się o 08:00, a kończy o 17:00. Kopie zapasowe danych użytkowników powinny być tworzone od razu po wylogowaniu się użytkowników, ale nie wcześniej niż o 16:30.

Kopie zapasowe serwerów firmy są tworzone codziennie o 23:00. Tworzenie kopii zapasowej danych użytkowników powinno zatem się zakończyć przed 23:00, aby zwolnić przepustowość sieci na potrzeby kopii zapasowych serwerów.

Tworzenie kopii zapasowej danych użytkowników zajmuje najwyżej godzinę, więc powinno się rozpocząć najpóźniej o 22:00. Jeśli użytkownik wciąż jest zalogowany w określonym przedziale czasu lub wyloguje się o dowolnej innej godzinie — tworzenie kopii zapasowej danych tego użytkownika powinno zostać pominięte.

- Zdarzenie: **Gdy użytkownik wyloguje się z systemu**. Określ konto użytkownika: **Dowolny użytkownik**.
- Warunek: **Mieści się w przedziale czasu** od **16:30** do **22:00**.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Pomiń zaplanowaną operację tworzenia kopii zapasowej.**

Wskutek tego:

- Jeśli użytkownik wyloguje się między 16:30 a 22:00, tworzenie kopii zapasowej rozpocznie się od razu.
- Jeśli użytkownik wyloguje się o dowolnej innej godzinie, tworzenie kopii zapasowej zostanie pominięte.

Oszczędzaj baterię

Ten warunek rozpoczęcia zapobiega utworzeniu kopii zapasowej, jeśli komputer (na przykład laptop lub tablet) nie jest podłączony do źródła zasilania. Wartość opcji Warunki rozpoczęcia tworzenia kopii zapasowych określa, czy pominięta operacja tworzenia kopii zapasowej rozpocznie się po podłączeniu komputera do źródła zasilania.

Dostępne są następujące opcje:

© Acronis International GmbH, 2003-2024

- **Nie uruchamiaj przy zasilaniu z baterii**
  Tworzenie kopii zapasowej rozpocznie się tylko wtedy, gdy komputer jest podłączony do źródła zasilania.
- **Uruchom przy zasilaniu z baterii, jeśli poziom naładowania przekracza**
  Tworzenie kopii zapasowej rozpocznie się, jeśli komputer jest podłączony do źródła zasilania lub poziom naładowania baterii przewyższa określoną wartość.

Przykład

Kopia zapasowa danych jest tworzona w każdy dzień roboczy o godzinie 21:00. Jeśli komputer nie jest podłączony do źródła zasilania, można pominąć tworzenie kopii zapasowej w celu oszczędzania energii akumulatora i poczekać na podłączenie komputera do źródła zasilania.

- Harmonogram: **Codziennie**, **Uruchamiaj od poniedziałku do piątku**. Uruchom o: **21:00**.
- Warunek: **Oszczędzaj baterię**, **Nie uruchamiaj przy zasilaniu z baterii**.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Poczekaj na spełnienie warunków**.

Wskutek tego:

- Jeśli o godzinie 21:00 komputer będzie podłączony do źródła zasilania, tworzenie kopii zapasowej rozpocznie się od razu.
- Jeśli o godzinie 21:00 komputer będzie działać na zasilaniu z akumulatora, tworzenie kopii zapasowej rozpocznie się dopiero po podłączeniu komputera do źródła zasilania.

Nie uruchamiaj przy połączeniu taryfowym

Użyj tego warunku rozpoczęcia, aby zapobiec utworzeniu kopii zapasowej (w tym kopii zapasowej dysku lokalnego), jeśli komputer ma połączenie z Internetem przez połączenie skonfigurowane w systemie Windows jako taryfowe. Aby uzyskać więcej informacji na temat połączeń taryfowych w systemie Windows, zobacz https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

Dodatkowy warunek rozpoczęcia **Nie uruchamiaj przy połączeniu z następującymi sieciami Wi-Fi** zostanie automatycznie włączony, jeśli włączysz warunek **Nie uruchamiaj przy połączeniu taryfowym**. Jest to dodatkowy środek zapobiegający tworzeniu kopii zapasowych za pośrednictwem hotspotów z telefonów komórkowych. Domyślnie są określone następujące nazwy sieci: android, telefon, komórka i modem.

Aby usunąć te nazwy z listy, kliknij symbol X. Aby dodać nową nazwę, wpisz ją w pustym polu.

Przykład

Kopia zapasowa danych jest tworzona w każdy dzień roboczy o godzinie 21:00. Jeśli komputer ma połączenie z Internetem przy użyciu połączenia taryfowego, można pominąć operację tworzenia kopii zapasowej, aby zredukować ruch w sieci, i poczekać na zaplanowane rozpoczęcie tej operacji w następnym dniu roboczym.

© Acronis International GmbH, 2003-2024

- Harmonogram: **Codziennie**, **Uruchamiaj od poniedziałku do piątku**. Uruchom o: **21:00**.
- Warunek: **Nie uruchamiaj przy połączeniu taryfowym**.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Pomiń zaplanowaną operację tworzenia kopii zapasowej.**

Wskutek tego:

- Jeśli o godzinie 21:00 komputer nie jest połączony z Internetem przy użyciu połączenia taryfowego, tworzenie kopii zapasowej rozpocznie się od razu.
- Jeśli o godzinie 21:00 komputer jest połączony z Internetem przy użyciu połączenia taryfowego, tworzenie kopii zapasowej rozpocznie się w następnym dniu roboczym.
- Jeśli o godzinie 21:00 w dni robocze komputer zawsze jest połączony z Internetem przy użyciu połączenia taryfowego, tworzenie kopii zapasowej w ogóle się nie rozpocznie.

Nie uruchamiaj przy połączeniu z następującymi sieciami Wi-Fi

Użyj tego warunku rozpoczęcia, aby zapobiec utworzeniu kopii zapasowej (w tym kopii zapasowej na dysku lokalnym), jeśli komputer jest połączony z dowolną ze wskazanych sieci bezprzewodowych (na przykład wtedy, gdy zechcesz ograniczyć tworzenie kopii zapasowych za pośrednictwem hotspota z telefonu komórkowego).

Można określić nazwy sieci Wi-Fi, znane również jako identyfikatory SSID. Ograniczenie to ma zastosowanie do wszystkich sieci mających w nazwie określony ciąg znaków (wielkość liter nie jest rozróżniana). Jeśli na przykład podasz nazwę sieci `phone`, tworzenie kopii zapasowej się nie rozpocznie, gdy urządzenie jest podłączone do jednej z następujących sieci: `John's iPhone`, `phone_wifi` lub `my_PHONE_wifi`.

Warunek rozpoczęcia **Nie uruchamiaj przy połączeniu z następującymi sieciami Wi-Fi** zostanie automatycznie włączony, jeśli włączysz warunek **Nie uruchamiaj przy połączeniu taryfowym**. Domyślnie są określone następujące nazwy sieci: android, `telefon`, `komórka` i modem.

Aby usunąć te nazwy z listy, kliknij symbol X. Aby dodać nową nazwę, wpisz ją w pustym polu.

Przykład

Kopia zapasowa danych jest tworzona w każdy dzień roboczy o godzinie 21:00. Jeśli komputer ma połączenie z Internetem za pośrednictwem hotspota z telefonu komórkowego, chcesz pominąć operację tworzenia kopii zapasowej i poczekać na zaplanowane rozpoczęcie takiej operacji w następnym dniu roboczym.

- Harmonogram: **Codziennie**, **Uruchamiaj od poniedziałku do piątku**. Uruchom o: **21:00**.
- Warunek: **Nie uruchamiaj przy połączeniu z następującymi sieciami**, **Nazwa sieci**: `<SSID sieci hotspota>`.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Pomiń zaplanowaną operację tworzenia kopii zapasowej.**

Wskutek tego:

© Acronis International GmbH, 2003-2024

- Jeśli o godzinie 21:00 komputer nie jest połączony z określoną siecią, tworzenie kopii zapasowej rozpocznie się od razu.
- Jeśli o godzinie 21:00 komputer jest połączony z określoną siecią, tworzenie kopii zapasowej rozpocznie się w następnym dniu roboczym.
- Jeśli o godzinie 21:00 w dni robocze komputer zawsze jest połączony z określoną siecią, tworzenie kopii zapasowej w ogóle się nie rozpocznie.

Sprawdź adres IP urządzenia

Ten warunek rozpoczęcia umożliwia zapobieżenie utworzeniu kopii zapasowej (w tym kopii zapasowej dysku lokalnego), jeśli którykolwiek z adresów IP komputera znajduje się w określonym zakresie adresów IP lub poza nim. W ten sposób można na przykład uniknąć dużych opłat za przesyłanie danych w przypadku tworzenia kopii zapasowych komputerów użytkowników przebywających za granicą lub zapobiec tworzeniu kopii zapasowych za pośrednictwem połączenia wirtualnej sieci prywatnej (VPN).

Dostępne są następujące opcje:

- **Uruchom, jeśli jest spoza zakresu adresów IP**
- **Uruchom, jeśli jest w zakresie adresów IP**

W przypadku każdej z tych opcji można określić kilka zakresów. Obsługiwane są tylko adresy IPv4.

Przykład

Kopia zapasowa danych jest tworzona w każdy dzień roboczy o godzinie 21:00. Jeśli komputer jest podłączony do sieci firmowej przez tunel VPN, ma zostać pominięta operacja tworzenia kopii zapasowej.

- Harmonogram: **Codziennie**, **Uruchamiaj od poniedziałku do piątku**. Początek o **21:00**.
- Warunek: **Sprawdź adres IP urządzenia**, **Uruchom, jeśli jest spoza zakresu adresów IP**, **Od**: `<początek zakresu adresów IP sieci VPN>`, **Do**: `<konie zakresu adresów IP sieci VPN>`.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Poczekaj na spełnienie warunków**.

Wskutek tego:

- Jeśli o godzinie 21:00 adres IP komputera nie znajduje się w określonym zakresie, tworzenie kopii zapasowej rozpocznie się od razu.
- Jeśli o godzinie 21:00 adres IP komputera znajduje się w określonym zakresie, tworzenie kopii zapasowej rozpocznie się dopiero wtedy, gdy komputer uzyska adres IP spoza sieci VPN.
- Jeśli o godzinie 21:00 w dni robocze adres IP komputera zawsze znajduje się w podanym zakresie, tworzenie kopii zapasowej w ogóle nie zostanie rozpoczęte.

Dodatkowe opcje planowania

Operacje tworzenia kopii zapasowych można skonfigurować tak, aby były uruchamiane tylko wtedy, gdy są spełnione określone warunki, tylko we wskazanym okresie lub z opóźnieniem w stosunku do

© Acronis International GmbH, 2003-2024

harmonogramu.

Aby skonfigurować warunki rozpoczęcia

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. Kliknij **Harmonogram**.
3. W panelu **Harmonogram** kliknij **Pokaż więcej**.
4. Zaznacz pola wyboru obok warunków rozpoczęcia, które chcesz uwzględnić, a następnie kliknij **Gotowe**.
   Dodatkowe informacje na temat dostępnych warunków rozpoczęcia i instrukcje dotyczące ich konfigurowania można znaleźć w sekcji "Warunki rozpoczęcia" (s. 457).
5. Zapisz plan ochrony.

Aby skonfigurować zakres czasu

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. Kliknij **Harmonogram**.
3. Zaznacz pole wyboru **Uruchom plan w danym przedziale dat**.
4. Wybierz odstęp czasowy stosownie do potrzeb, a następnie kliknij **Gotowe**.
5. Zapisz plan ochrony.

W wyniku tych działań operacje tworzenia kopii zapasowych będą uruchamiane tylko we wskazanym okresie.

Aby skonfigurować opóźnienie

Aby uniknąć nadmiernego obciążenia sieci podczas tworzenia kopii zapasowych wielu obciążeń w lokalizacji sieciowej, jako opcję tworzenia kopii zapasowych skonfigurowano niewielkie losowe opóźnienie. Można je wyłączyć lub zmienić jego ustawienia.

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. Kliknij **Opcje tworzenia kopii zapasowych**, a następnie wybierz **Tworzenie harmonogramu**.
   Wartość opóźnienia jest w przypadku każdego obciążenia wybierana losowo z zakresu od zera do określonej przez Ciebie wartości maksymalnej. Domyślnie wartością maksymalną jest 30 minut.
   Dodatkowe informacje na temat tej opcji tworzenia kopii zapasowych można znaleźć w sekcji "Tworzenie harmonogramu" (s. 524)
   Wartość opóźnienia w przypadku każdego obciążenia jest obliczana po zastosowaniu planu ochrony do tego obciążenia i pozostaje taka sama do czasu, aż zostanie edytowana maksymalna wartość opóźnienia.
3. Wybierz odstęp czasowy stosownie do potrzeb, a następnie kliknij **Gotowe**.
4. Zapisz plan ochrony.

© Acronis International GmbH, 2003-2024

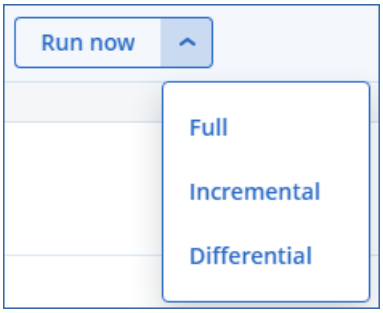
Ręczne uruchamianie operacji tworzenia kopii zapasowej

Operacje tworzenia kopii zapasowej — zarówno te zaplanowane, jak i niezaplanowane — można uruchamiać ręcznie.

Aby ręcznie uruchomić operację tworzenia kopii zapasowej

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Wybierz obciążenie, w odniesieniu do którego chcesz uruchomić operację tworzenia kopii zapasowej, a następnie kliknij **Chroń**.
3. Wybierz plan ochrony, przy użyciu którego chcesz utworzyć kopię zapasową.
   Jeśli do obciążenia nie zastosowano żadnego planu ochrony, zastosuj już istniejący plan lub utwórz nowy.
   Dokładniejsze instrukcje dotyczące tworzenia planu ochrony można znaleźć w sekcji "Tworzenie planu ochrony" (s. 222).
4. [Aby utworzyć domyślny typ kopii zapasowej] W planie ochrony kliknij ikonę **Uruchom teraz**.

   Możesz też rozwinąć w planie ochrony moduł **Kopia zapasowa** i kliknąć przycisk **Uruchom teraz**.
5. [Aby utworzyć określony typ kopii zapasowej] W planie ochrony rozwiń moduł **Kopia zapasowa**, kliknij strzałkę przy przycisku **Uruchom teraz** i wybierz typ kopii zapasowej.

   Uwaga
   Wybór typu nie jest dostępny w przypadku schematów tworzenia kopii zapasowych obejmujących tylko jedną metodę tworzenia kopii zapasowej, na przykład **Zawsze przyrostowa (jednoplikowa)** lub **Zawsze pełne**.

W wyniku tych działań rozpocznie się operacja tworzenia kopii zapasowej. Jej postęp i wyniki możesz sprawdzać na karcie **Urządzenia**, w kolumnie **Status**.

© Acronis International GmbH, 2003-2024

Reguły przechowywania

Aby starsze kopie zapasowe były usuwane automatycznie, należy skonfigurować reguły przechowywania kopii zapasowych w planie ochrony.

Reguły przechowywania można oprzeć na dowolnej z poniższych właściwości kopii zapasowych:

- Numer
- Wiek
- Rozmiar

Dostępne reguły przechowywania i ich opcje zależą od schematu tworzenia kopii zapasowych. Reguły te dotyczą również agentów, obciążeń i kopii zapasowych z chmury do chmury. Aby uzyskać więcej informacji, zobacz "Reguły przechowywania zgodnie ze schematem tworzenia kopii zapasowych" (s. 468).

W zależności od konfiguracji planu ochrony reguły przechowywania są stosowane do archiwum przed utworzeniem kopii zapasowej lub po jej utworzeniu.

Automatyczne czyszczenie starszych kopii zapasowych można wyłączyć, wybierając opcję **Przechowuj kopie zapasowe bezterminowo** podczas konfigurowania reguł przechowywania. Może to powodować zajmowanie większej ilości miejsca w pamięci masowej i konieczność ręcznego usuwania niepotrzebnych starych kopii zapasowych.

Ważne wskazówki

- Reguły przechowywania stanowią część planu ochrony. Jeśli plan zostanie odwołany lub usunięty, reguły przechowywania zdefiniowane w tym planie nie będą już stosowane. Dokładniejsze instrukcje dotyczące usuwania niepotrzebnych już kopii zapasowych można znaleźć w sekcji "Usuwanie kopii zapasowych" (s. 572).
- Jeśli zgodnie ze schematem tworzenia kopii zapasowych i formatem kopii zapasowych każda kopia zapasowa jest przechowywana jako oddzielny plik, to kopia zapasowa, od której zależą jakieś przyrostowe lub różnicowe kopie zapasowe, nie może zostać usunięta. Taka kopia zostanie usunięta zgodnie z regułami przechowywania zastosowanymi do zależnych kopii zapasowych. Taka konfiguracja może powodować zajmowanie większej ilości miejsca w pamięci masowej w związku z opóźnieniem usunięcia niektórych kopii zapasowych. Ponadto określone wartości mogą zostać przekroczone ze względu na wiek, liczbę lub rozmiar kopii zapasowych. Dokładniejsze instrukcje dotyczące zmieniania tego zachowania można znaleźć w sekcji "Konsolidacja kopii zapasowych" (s. 482).
- Domyślnie najnowsza kopia zapasowa utworzona w ramach planu ochrony nigdy nie jest usuwana. Jeśli jednak skonfigurujesz regułę przechowywania wymagającą wyczyszczenia kopii zapasowych przed rozpoczęciem nowej operacji tworzenia kopii zapasowej i ustawisz liczbę zachowywanych kopii zapasowych jako zero, to zostanie usunięta również najnowsza kopia zapasowa.

© Acronis International GmbH, 2003-2024

Ostrzeżenie!
Jeśli zastosujesz tę regułę przechowywania do zestawu kopii zapasowych z jedną kopią zapasową, a operacja tworzenia kopii zapasowej się nie powiedzie, nie będziesz w stanie odzyskać danych, ponieważ istniejąca już kopia zapasowa zostanie usunięta, nim zostanie utworzona nowa.

Reguły przechowywania zgodnie ze schematem tworzenia kopii zapasowych

Dostępne reguły przechowywania i ich ustawienia zależą od schematu tworzenia kopii zapasowych używanego w planie ochrony. Dodatkowe informacje na temat schematów tworzenia kopii zapasowych można znaleźć w sekcji "Schematy tworzenia kopii zapasowych" (s. 447).

W poniższej tabeli zestawiono dostępne reguły przechowywania i ich ustawienia.

Schemat tworzenia kopii zapasowych	Harmonogram	Dostępne reguły przechowywania i ich ustawienia
Zawsze przyrostowa (jednoplikowa)	Co miesiąc Co tydzień Codziennie Co godzinę Operacje tworzenia kopii zapasowych wyzwalane przez zdarzenia	Według liczby kopii zapasowych Według wieku kopii zapasowych (osobne ustawienia dla miesięcznych, tygodniowych, dziennych i godzinowych kopii zapasowych) Przechowuj kopie zapasowe bezterminowo
Zawsze pełne	Co miesiąc Co tydzień Codziennie Co godzinę Operacje tworzenia kopii zapasowych wyzwalane przez zdarzenia	Według liczby kopii zapasowych Według wieku kopii zapasowych (osobne ustawienia dla miesięcznych, tygodniowych, dziennych i godzinowych kopii zapasowych) Według łącznego rozmiaru kopii zapasowych Przechowuj kopie zapasowe bezterminowo
Tygodniowe pełne, dzienne przyrostowe	Codziennie Operacje tworzenia kopii zapasowych wyzwalane przez zdarzenia	Według liczby kopii zapasowych Według wieku kopii zapasowych (osobne ustawienia dla tygodniowych i dziennych kopii zapasowych) Według łącznego rozmiaru kopii zapasowych Przechowuj kopie zapasowe bezterminowo

© Acronis International GmbH, 2003-2024

Schemat tworzenia kopii zapasowych	Harmonogram	Dostępne reguły przechowywania i ich ustawienia
Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe	Co miesiąc Co tydzień Codziennie Co godzinę Operacje tworzenia kopii zapasowych wyzwalane przez zdarzenia	Według liczby kopii zapasowych Według wieku kopii zapasowych (osobne ustawienia dla pełnych, różnicowych i przyrostowych kopii zapasowych) Według łącznego rozmiaru kopii zapasowych Przechowuj kopie zapasowe bezterminowo
Niestandardowe	Co miesiąc Co tydzień Codziennie Co godzinę Operacje tworzenia kopii zapasowych wyzwalane przez zdarzenia	Według liczby kopii zapasowych Według wieku kopii zapasowych (osobne ustawienia dla pełnych, różnicowych i przyrostowych kopii zapasowych) Według łącznego rozmiaru kopii zapasowych Przechowuj kopie zapasowe bezterminowo

Dlaczego istnieją miesięczne kopie zapasowe ze schematem godzinowym?

W zależności od schematu tworzenia kopii zapasowych można skonfigurować opcję **Według wieku kopii zapasowych** dla jednej z następujących kopii zapasowych:

- miesięczna, tygodniowa, dzienna i godzinowa kopia zapasowa.

  Ustawienia te są dostępne we wszystkich schematach tworzenia kopii zapasowych niebędących schematami niestandardowymi i dotyczą czasu. Wszystkie te kopie zapasowe (miesięczne, tygodniowe, dzienne i godzinowe) są dostępne nawet wtedy, gdy zostanie skonfigurowane uruchamianie operacji tworzenia kopii zapasowych co godzinę. Zapoznaj się z poniższym przykładem.

Kopia zapasowa	Opis
Co miesiąc	Miesięczną kopią zapasową jest pierwsza kopia zapasowa utworzona w każdym miesiącu.
Co tydzień	Tygodniową kopią zapasową jest pierwsza kopia zapasowa w dniu tygodnia wybranym w polu Tygodniowa kopia zapasowa. Ten dzień jest uznawany za początek tygodnia z perspektywy reguł przechowywania. Jeśli tygodniowa kopia zapasowa jest też pierwszą kopią zapasową utworzoną w danym miesiącu, jest ona uznawana za miesięczną kopię zapasową. W takiej sytuacji tygodniowa kopia zapasowa zostanie

© Acronis International GmbH, 2003-2024

Kopia zapasowa	Opis
	utworzona w wybrany dzień następnego tygodnia.
Codziennie	Dzienną kopią zapasową jest pierwsza kopia zapasowa utworzona w danym dniu, chyba że spełnia warunki definicji miesięcznej lub tygodniowej kopii zapasowej. W takiej sytuacji dzienna kopia zapasowa zostanie utworzona w następnego dnia.
Co godzinę	Godzinową kopią zapasową jest pierwsza kopia zapasowa utworzona w ramach danej godziny, chyba że spełnia warunki definicji miesięcznej, tygodniowej lub dziennej kopii zapasowej. W takiej sytuacji godzinowa kopia zapasowa zostanie utworzona w ciągu następnej godziny.

- Pełne, różnicowe i przyrostowe kopie zapasowe.

  Ustawienia te są dostępne w schemacie tworzenia kopii zapasowych **Niestandardowe** i zależą od metody tworzenia kopii zapasowych. Schemat tworzenia kopii zapasowych **Miesięczna pełna, tygodniowa różnicowa, dzienna przyrostowa** jest fabrycznie skonfigurowanym specjalnym schematem.

Przykład

Używasz schematu tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** z domyślnym ustawieniem godzinowych kopii zapasowych:

- Zaplanowane według czasu.
- Operacje tworzenia kopii zapasowych uruchamiane co godzinę: Od poniedziałku do piątku, co godzinę, między 08:00 a 18:00.
- Opcja **Tygodniowa kopia zapasowa** ma ustawioną wartość Poniedziałek.

W sekcji **Okres przechowywania** planu ochrony można zastosować reguły przechowywania do miesięcznych, tygodniowych, dziennych i godzinowych kopii zapasowych.

W poniższej tabeli zestawiono typy kopii zapasowych tworzonych w ciągu 8 dni.

Data	Dzień tygodnia	Opis
1 lipca	Poniedziałek	Pierwsza kopia zapasowa każdego miesiąca jest kopią miesięczną, a zatem pierwsza kopia zapasowa w tym dniu jest kopią miesięczną. Pozostałe kopie zapasowe utworzone w tym dniu są kopiami godzinowymi. Pierwsza kopia zapasowa w tym tygodniu jest uznawana za kopię miesięczną. Dlatego nie ma tygodniowej kopii zapasowej. Kopią tygodniową będzie pierwsza kopia zapasowa utworzona w następnym tygodniu.
2 lipca	Wtorek	Pierwsza kopia zapasowa jest kopią dzienną, a pozostałe kopie zapasowe utworzone w tym dniu są kopiami godzinowymi.

© Acronis International GmbH, 2003-2024

Data	Dzień tygodnia	Opis
3 lipca	Środa	Pierwsza kopia zapasowa jest kopią dzienną, a pozostałe kopie zapasowe utworzone w tym dniu są kopiami godzinowymi.
4 lipca	Czwartek	Pierwsza kopia zapasowa jest kopią dzienną, a pozostałe kopie zapasowe utworzone w tym dniu są kopiami godzinowymi.
5 lipca	Piątek	Pierwsza kopia zapasowa jest kopią dzienną, a pozostałe kopie zapasowe utworzone w tym dniu są kopiami godzinowymi.
6 lipca	Sobota	Pierwsza kopia zapasowa jest kopią dzienną, a pozostałe kopie zapasowe utworzone w tym dniu są kopiami godzinowymi.
7 lipca	Niedziela	Pierwsza kopia zapasowa jest kopią dzienną, a pozostałe kopie zapasowe utworzone w tym dniu są kopiami godzinowymi.
8 lipca	Poniedziałek	Pierwsza kopia zapasowa jest kopią tygodniową, a pozostałe kopie zapasowe utworzone w tym dniu są kopiami godzinowymi.

Konfigurowanie reguł przechowywania

Reguły przechowywania stanowią część planu ochrony, a ich dostępność i opcje zależą od schematu tworzenia kopii zapasowych. Aby uzyskać więcej informacji, zobacz "Reguły przechowywania zgodnie ze schematem tworzenia kopii zapasowych" (s. 468).

Aby skonfigurować reguły przechowywania

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. Kliknij **Liczba przechowywanych**.
3. Wybierz jedną z następujących opcji:
   - **Według liczby kopii zapasowych**
   - **Według wieku kopii zapasowych**

     Dostępne są osobne ustawienia dla miesięcznych, tygodniowych, dziennych i godzinowych kopii zapasowych. W przypadku każdego typu wartością maksymalną jest 9999.

     Można też użyć jednego ustawienia w odniesieniu do wszystkich kopii zapasowych.
   - **Według łącznego rozmiaru kopii zapasowych**

     To ustawienie jest niedostępne w przypadku schematu tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)**.
   - **Przechowuj kopie zapasowe bezterminowo**
4. [Jeśli nie wybrano opcji **Przechowuj kopie zapasowe bezterminowo**] Skonfiguruj wartości dla wybranej opcji.
5. [Jeśli nie wybrano opcji **Przechowuj kopie zapasowe bezterminowo**] Określ, kiedy mają być stosowane reguły przechowywania:

© Acronis International GmbH, 2003-2024

- Po utworzeniu kopii zapasowej
- Przed utworzeniem kopii zapasowej

  Ta opcja jest niedostępna w przypadku tworzenia kopii zapasowych klastrów programu Microsoft SQL Server lub Microsoft Exchange Server.

6. Kliknij **Gotowe**.
7. Zapisz plan ochrony.

Replikacja

W przypadku włączenia replikacji każda nowa kopia zapasowa jest automatycznie kopiowana do lokalizacji replikacji. Kopie zapasowe w lokalizacji replikacji są niezależne od kopii zapasowych pozostałych w lokalizacji źródłowej — i na odwrót.

Replikowana jest tylko ostatnia kopia zapasowa dostępna w lokalizacji źródłowej. Jeśli jednak wcześniejsze kopie zapasowe nie zostały zreplikowane (na przykład z powodu problemu z połączeniem sieciowym), operacja replikacji obejmie wszystkie kopie zapasowe utworzone po ostatniej udanej replikacji.

Jeśli operacja replikacji zostanie przerwana, przetworzone dane zostaną wykorzystane podczas następnej operacji replikacji.

Uwaga
W tym temacie opisano replikację jako część planu ochrony. Można także utworzyć oddzielny plan replikacji kopii zapasowych. Aby uzyskać więcej informacji, zobacz "Replikacja kopii zapasowej" (s. 230).

Przykłady użycia

- Zapewnianie niezawodnego odzyskiwania

  Kopie zapasowe należy przechowywać zarówno lokalnie (aby mieć możliwość natychmiastowego odzyskania danych), jak i w innej lokalizacji (aby mieć pewność, że te kopie zapasowe pozostaną bezpieczne nawet w przypadku awarii lub klęski żywiołowej powodującej szkody w lokalizacji podstawowej).
- Korzystanie z chmury w celu ochrony danych przed skutkami klęsk żywiołowych

  Istnieje możliwość replikowania kopii zapasowych do chmury przez przesyłanie jedynie zmienionych danych.
- Przechowywanie jedynie ostatnich punktów odzyskiwania

  Skonfiguruj reguły przechowywania, aby starsze kopie zapasowe były usuwane z szybkiej pamięci masowej, co pozwoli zaoszczędzić na kosztach przechowywania.

© Acronis International GmbH, 2003-2024

Obsługiwane lokalizacje

Lokalizacja	Jako lokalizacja źródłowa	Jako lokalizacja replikacji
Folder lokalny	+	+
Folder sieciowy	+	+
Chmura	-	+
Secure Zone	+	–
Chmura publiczna	+	+

W celu włączenia replikacji

1. W planie ochrony rozwiń moduł **Kopia zapasowa**, a następnie kliknij **Dodaj lokalizację**.

   Uwaga
   Opcja **Dodaj lokalizację** nie jest dostępna w przypadku wybrania chmury w sekcji **Miejsce docelowe kopii zapasowej**.

2. Wybierz lokalizację replikacji z listy dostępnych lokalizacji.
   Lokalizacja ta jest pokazywana w planie ochrony jako **Druga lokalizacja**, **Trzecia lokalizacja**, **Czwarta lokalizacja** lub **Piąta lokalizacja**, w zależności od liczby lokalizacji dodanych na potrzeby replikacji.
3. [Opcjonalnie] Kliknij ikonę koła zębatego, aby skonfigurować opcje lokalizacji replikacji.
   - **Wydajność i okno na utworzenie kopii zapasowej** — skonfiguruj okno na utworzenie kopii zapasowej dla wybranej lokalizacji zgodnie z opisem podanym w sekcji "Wydajność i okno na utworzenie kopii zapasowej" (s. 513). Te ustawienia decydują o wydajności replikacji.
   - **Usuń lokalizację** — usuń aktualnie wybraną lokalizację replikacji.
   - [Tylko w przypadku chmury] **Fizyczne dostarczanie danych** — zapisz początkową kopię zapasową na wymiennym urządzeniu pamięci masowej i dostarcz ją w celu przesłania do chmury zamiast replikowania przez Internet.
     Ta opcja jest odpowiednia w przypadku lokalizacji z wolnym połączeniem sieciowym lub jeśli nie chcesz obciążać łącza przesyłaniem dużych plików przez sieć. Włączenie tej opcji nie wymaga zaawansowanych limitów usługi Cyber Protect, ale do utworzenia zlecenia wysyłki i śledzenia go potrzebny będzie limit usługi Fizyczne dostarczanie danych. Zobacz "Fizyczne dostarczanie danych" (s. 517).

     Uwaga
     Ta opcja jest obsługiwana w przypadku agenta ochrony w wersji C21.06 lub nowszej.

4. [Opcjonalnie] W wierszu **Liczba przechowywanych** w obszarze lokalizacji replikacji skonfiguruj reguły przechowywania dla tej lokalizacji zgodnie z opisem podanym w sekcji "Reguły przechowywania" (s. 467).

© Acronis International GmbH, 2003-2024

5. [Opcjonalnie] Powtarzaj kroki 1–4, aby dodać więcej lokalizacji replikacji.

   Możesz skonfigurować maksymalnie cztery lokalizacje replikacji (**Druga lokalizacja**, **Trzecia lokalizacja**, **Czwarta lokalizacja** i **Piąta lokalizacja**). W przypadku wybrania opcji **Chmura** nie możesz dodać więcej lokalizacji replikacji.

Ważne

W przypadku włączenia tworzenia kopii zapasowych i replikacji w tym samym planie ochrony należy dopilnować, aby replikacja została zakończona przed uruchomieniem następnej zaplanowanej operacji tworzenia kopii zapasowej. Jeśli replikacja wciąż jest w toku, zaplanowana operacja tworzenia kopii zapasowej nie zostanie uruchomiona, na przykład zaplanowana operacja tworzenia kopii zapasowej uruchamiana co 24 godziny nie zostanie uruchomiona, jeśli replikacja potrwa 26 godzin.

Aby uniknąć takiej zależności, należy użyć oddzielnego planu na potrzeby replikacji kopii zapasowych. Więcej informacji na temat tego konkretnego planu można znaleźć w sekcji "Replikacja kopii zapasowej" (s. 230).

Szyfrowanie

Algorytm kryptograficzny Advanced Encryption Standard (AES) działa w trybie Galois/Counter (GCM) i używa losowo generowanego 256-bitowego klucza. Następnie klucz szyfrowania jest szyfrowany za pomocą algorytmu AES-256 przy użyciu skrótu SHA-2 (256-bitowego) hasła jako klucza. Samo hasło nie jest zapisywane nigdzie na dysku ani w kopii zapasowej, a skrót hasła służy do weryfikacji.

W przypadku zastosowania takiej dwupoziomowej ochrony dane kopii zapasowej są chronione przed nieuprawnionym dostępem, ale nie można odzyskać utraconego hasła.

Uwaga

Korzystanie z algorytmu AES-256 z silnym hasłem zapewnia szyfrowanie odporne na poziomie kwantowym. Jest ono skuteczne w przypadku ataków kryptograficznych opartych na obliczeniach kwantowych.

Zalecamy szyfrowanie wszystkich kopii zapasowych przechowywanych w chmurze, zwłaszcza jeśli firma podlega obowiązkowi zachowania zgodności ze stosownymi przepisami.

Szyfrowanie można skonfigurować na następujące sposoby:

- W planie ochrony
- Jako właściwość komputera, za pomocą narzędzia Cyber Protect Monitor lub interfejsu wiersza polecenia

Konfigurowanie szyfrowania w planie ochrony

W planie ochrony szyfrowanie jest domyślnie włączone. Stosowany jest algorytm AES-256.

Dzięki silnemu hasłu algorytm AES-256 zapewnia szyfrowanie odporne na ataki oparte na obliczeniach kwantowych.

© Acronis International GmbH, 2003-2024

W przypadku kont w trybie zgodności nie można konfigurować szyfrowania w planie ochrony. Aby uzyskać więcej informacji na temat konfigurowania szyfrowania na chronionym urządzeniu, zobacz sekcję "Konfigurowanie szyfrowania jako właściwości komputera" (s. 475).

Aby skonfigurować szyfrowanie

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. W sekcji **Szyfrowaniu** kliknij **Określ hasło**.
3. Określ i potwierdź hasło szyfrowania.
4. Kliknij **OK**.

Ostrzeżenie!
W przypadku zgubienia lub zapomnienia hasła nie da się odzyskać zaszyfrowanych kopii zapasowych.

Po zastosowaniu planu ochrony nie można zmienić ustawień szyfrowania. Aby użyć innych ustawień szyfrowania, utwórz nowy plan.

Konfigurowanie szyfrowania jako właściwości komputera

Możesz skonfigurować szyfrowanie kopii zapasowej jako właściwość komputera. W tym przypadku szyfrowanie kopii zapasowej nie jest konfigurowane w planie ochrony, ale na chronionym obciążeniu. Szyfrowanie jako właściwość komputera jest wykonywane przy użyciu algorytmu AES z kluczem 256-bitowym (AES-256).

Uwaga
Korzystanie z algorytmu AES-256 z silnym hasłem zapewnia szyfrowanie odporne na poziomie kwantowym. Jest ono skuteczne w przypadku ataków kryptograficznych opartych na obliczeniach kwantowych.

Skonfigurowanie szyfrowania jako właściwości komputera wpływa na plany ochrony w następujący sposób:

- **Plany ochrony już zastosowane do komputera.** Jeśli ustawienia szyfrowania w planie ochrony są inne, nie uda się utworzyć kopii zapasowych.
- **Plany ochrony, które zostaną później zastosowane na komputerze.** Ustawienia szyfrowania zapisane na komputerze zastąpią ustawienia szyfrowania zawarte w planie ochrony. Każda kopia zapasowa zostanie zaszyfrowana, nawet jeśli szyfrowanie jest wyłączone w ustawieniach modułu Kopia zapasowa.

W przypadku kont w trybie zgodności dostępne jest tylko szyfrowanie jako właściwość komputera.

Jeśli masz więcej niż jednego agenta dla VMware podłączonego do tego samego serwera vCenter i skonfigurujesz szyfrowanie jako właściwość komputera, musisz używać tego samego hasła szyfrowania na wszystkich komputerach z agentem dla VMware ze względu na równoważenie obciążenia między agentami.

© Acronis International GmbH, 2003-2024

Możesz skonfigurować szyfrowanie jako właściwość komputera w następujący sposób:

- W wierszu polecenia
- W narzędziu Cyber Protect Monitor (dostępnym w systemie Windows i macOS)

Aby skonfigurować szyfrowanie

W wierszu polecenia

1. Zaloguj się jako administrator (w systemie Windows) lub użytkownik root (w systemie Linux).
2. W wierszu polecenia uruchom następujące polecenie:
   - W przypadku systemu Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
     <encryption_password>
     ```

     Domyślnie ścieżka instalacji jest następująca: `%ProgramFiles%\BackupClient`.
   - W przypadku systemu Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   - W przypadku urządzenia wirtualnego:

     ```
      /./sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   Ostrzeżenie!
   W przypadku zgubienia lub zapomnienia hasła nie da się odzyskać zaszyfrowanych kopii zapasowych.

W narzędziu Cyber Protect Monitor

1. Zaloguj się jako administrator.
2. Kliknij ikonę narzędzia Cyber Protect Monitor w obszarze powiadomień (w systemie Windows) lub na pasku menu (w systemie macOS).
3. Kliknij ikonę koła zębatego, a następnie kliknij **Ustawienia** > **Szyfrowanie**.
4. Wybierz **Ustaw hasło dla tego komputera**. Podaj i potwierdź hasło szyfrowania.
5. Kliknij **Zapisz**.

Ostrzeżenie!
W przypadku zgubienia lub zapomnienia hasła nie da się odzyskać zaszyfrowanych kopii zapasowych.

Aby zresetować ustawienia szyfrowania

1. Zaloguj się jako administrator (w systemie Windows) lub użytkownik root (w systemie Linux).
2. W wierszu polecenia uruchom następujące polecenie:

© Acronis International GmbH, 2003-2024

- W przypadku systemu Windows:

  ```
  <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
  ```

  Domyślnie ścieżka instalacji jest następująca: `%ProgramFiles%\BackupClient`.
- W przypadku systemu Linux:

  ```
  /usr/sbin/acropsh -m manage_creds --reset
  ```

- W przypadku urządzenia wirtualnego:

  ```
  /./sbin/acropsh -m manage_creds --reset
  ```

Ważne
Jeśli zresetujesz szyfrowanie jako właściwość komputera lub zmienisz hasło szyfrowania po utworzeniu kopii zapasowej przez plan ochrony, następna operacja tworzenia kopii zapasowej zakończy się niepowodzeniem. Aby kontynuować tworzenie kopii zapasowych obciążenia, utwórz nowy plan ochrony.

Notaryzacja

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Notaryzacja pozwala udowodnić, że plik jest autentyczny i niezmieniony od momentu uwzględnienia w kopii zapasowej. Notaryzację warto włączyć w przypadku tworzenia kopii zapasowej plików dokumentów prawnych lub innych plików, które wymagają potwierdzenia autentyczności.

Notaryzacja jest dostępna tylko w przypadku kopii zapasowych na poziomie plików. Pliki z podpisem cyfrowym są pomijane, ponieważ nie trzeba ich notaryzować.

Notaryzacja *nie* jest dostępna w następujących sytuacjach:

- Jeśli format kopii zapasowej jest ustawiony jako **Wersja 11**
- Jeśli lokalizacją docelową kopii zapasowej jest strefa Secure Zone

Jak korzystać z funkcji notaryzacji

Aby włączyć notaryzację wszystkich plików wybranych do uwzględnienia w kopii zapasowej (z wyjątkiem plików z podpisem cyfrowym), włącz przełącznik **Notaryzacja** podczas tworzenia planu ochrony.

W ramach konfiguracji odzyskiwania notaryzowane pliki będą oznaczone specjalną ikoną i będzie można zweryfikować ich autentyczność.

© Acronis International GmbH, 2003-2024

Sposób działania

Podczas tworzenia kopii zapasowej agent oblicza kody skrótów uwzględnianych w kopii plików, buduje drzewo skrótów (na podstawie struktury folderów), zapisuje drzewo w kopii zapasowej, a następnie wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji zapisuje główne drzewo skrótów w bazie danych łańcucha bloków Ethereum, aby zapewnić, że ta wartość nie zostanie zmieniona.

Weryfikując autentyczność pliku, agent oblicza jego skrót, a następnie porównuje go ze skrótem przechowywanym w drzewie skrótów w kopii zapasowej. W przypadku niezgodności skrótów uznaje się, że plik nie jest autentyczny. W przeciwnym razie autentyczność plików jest gwarantowana przez drzewo skrótów.

Aby zweryfikować, czy samo drzewo skrótów nie zostało naruszone, agent wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji porównuje je z drzewem przechowywanym w bazie danych łańcucha bloków. Jeśli skróty są zgodne, wybrany plik otrzymuje gwarancję autentyczności. W przeciwnym razie program wyświetla komunikat, że plik nie jest autentyczny.

Domyślne opcje tworzenia kopii zapasowej

Domyślne wartości opcji tworzenia kopii zapasowej istnieją na poziomie firmy, jednostki i użytkownika. Konto jednostki lub użytkownika utworzone w ramach firmy lub jednostki dziedziczy wartości domyślne ustawione dla tej firmy lub jednostki.

Administratorzy firmy, administratorzy jednostki i każdy użytkownik niemający praw administratora mogą zmienić domyślną wartość opcji na inną niż predefiniowana. Po wprowadzeniu zmiany nowa wartość będzie domyślnie używana we wszystkich planach ochrony utworzonych na danym poziomie.

Podczas tworzenia planu ochrony użytkownik może zastąpić wartość domyślną wartością niestandardową, która będzie używana tylko w ramach tego planu.

Aby zmienić domyślną wartość opcji

1. Wykonaj jedną z następujących czynności:
   - Aby zmienić wartość domyślną ustawioną dla firmy, zaloguj się do konsoli Cyber Protect jako administrator firmy.
   - Aby zmienić wartość domyślną ustawioną dla jednostki, zaloguj się do konsoli Cyber Protect jako administrator tej jednostki.
   - Aby zmienić wartość domyślną ustawioną dla siebie, zaloguj się do konsoli Cyber Protect przy użyciu konta, które nie ma praw administratora.
2. Kliknij **Ustawienia** > **Ustawienia systemowe**.
3. Rozwiń sekcję **Domyślne opcje tworzenia kopii zapasowych**.
4. Wybierz opcję, a następnie wprowadź wymagane zmiany.
5. Kliknij **Zapisz**.

© Acronis International GmbH, 2003-2024

Opcje tworzenia kopii zapasowych

Aby zmodyfikować opcje tworzenia kopii zapasowych w planie ochrony, w module **Kopia zapasowa** w polu **Opcje tworzenia kopii zapasowych** kliknij **Zmień**.

Dostępne opcje tworzenia kopii zapasowych

Zakres dostępnych opcji tworzenia kopii zapasowych zależy od następujących czynników:

- Środowisko działania agenta (Windows, Linux, macOS).
- Typ danych uwzględnianych w kopii zapasowej (dyski, pliki, maszyny wirtualne, dane aplikacji)
- Lokalizacja docelowa kopii zapasowej (chmura, folder lokalny lub sieciowy).

W poniższej tabeli zestawiono dostępność opcji tworzenia kopii zapasowych.

	Tworzenie kopii zapasowych na poziomie dysku			**Kopia zapasowa na poziomie plików**			**Maszyny wirtualne**			**SQL oraz Exchange**
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Windows**
Alerty	+	+	+	+	+	+	+	+	+	+
Konsolidacja kopii zapasowych	+	+	+	+	+	+	+	+	+	-
Nazwa pliku kopii zapasowej	+	+	+	+	+	+	+	+	+	+
Format kopii zapasowej	+	+	+	+	+	+	+	+	+	+
Sprawdzanie poprawności kopii zapasowej	+	+	+	+	+	+	+	+	+	+
CBT (Changed Block Tracking)	+	-	-	-	-	-	+	+	-	-
Tryb tworzenia kopii zapasowych klastra	-	-	-	-	-	-	-	-	-	+
Stopień kompresji	+	+	+	+	+	+	+	+	+	+
Obsługa błędów										
W razie błędu	+	+	+	+	+	+	+	+	+	+

© Acronis International GmbH, 2003-2024

spróbuj ponownie										
Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb cichy)	+	+	+	+	+	+	+	+	+	+
Ignoruj uszkodzone sektory	+	-	+	+	-	+	+	+	+	-
W razie błędu tworzenia migawki maszyny wirtualnej spróbuj ponownie	-	-	-	-	-	-	+	+	+	-
Szybka przyrostowa/różnicowa kopia zapasowa	+	+	+	-	-	-	-	-	-	-
Migawka kopii zapasowej na poziomie plików	-	-	-	+	+	+	-	-	-	-
Filtry plików	+	+	+	+	+	+	+	+	+	-
Dane do analizy śledczej	+	-	-	-	-	-	-	-	-	-
Obcinanie dziennika	-	-	-	-	-	-	+	+	-	Tylko SQL
Wykonywanie migawek LVM	-	+	-	-	-	-	-	-	-	-
Punkty zamontowania	-	-	-	+	-	-	-	-	-	-
Migawka wielowoluminowa	+	+	-	+	+	-	-	-	-	-
Odzyskiwanie jednym kliknięciem	+	+	-	-	-	-	-	-	-	-
Wydajność i okno na utworzenie kopii zapasowej	+	+	+	+	+	+	+	+	+	+
Fizyczne dostarczanie	+	+	+	+	+	+	+	+	+	-

© Acronis International GmbH, 2003-2024

danych										
Polecenia poprzedzające/następujące	+	+	+	+	+	+	+	+	+	+
Polecenia poprzedzające rejestrowanie danych/następujące po nim	+	+	+	+	+	+	-	-	-	+
Tworzenie harmonogramu										
Rozłóż uruchamianie w przedziale czasu	+	+	+	+	+	+	+	+	+	+
Ogranicz liczbę jednoczesnych operacji tworzenia kopii zapasowych	-	-	-	-	-	-	+	+	+	-
Kopia zapasowa sektor po sektorze	+	+	-	-	-	-	+	+	+	-
Dzielenie	+	+	+	+	+	+	+	+	+	+
Obsługa niepowodzenia zadania	+	+	+	+	+	+	+	+	+	+
Warunki uruchomienia zadania	+	+	-	+	+	-	+	+	+	+
Usługa kopiowania woluminów w tle (VSS)	+	-	-	+	-	-	-	+	-	+
Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych	-	-	-	-	-	-	+	+	-	-
Tygodniowa kopia zapasowa	+	+	+	+	+	+	+	+	+	+
Dziennik zdarzeń systemu Windows	+	-	-	+	-	-	+	+	-	+

© Acronis International GmbH, 2003-2024

Alerty

Brak pomyślnie utworzonych kopii zapasowych przez określoną liczbę kolejnych dni

Ustawienie wstępne: **Wyłączono**.

Ta opcja pozwala określić, czy oprogramowanie ma wygenerować alert, jeśli przez określony czas w ramach planu ochrony nie zostanie utworzona pomyślnie ani jedna kopia zapasowa. Oprócz nieudanych operacji tworzenia kopii zapasowych oprogramowanie zlicza kopie zapasowe, które nie zostały uruchomione zgodnie z harmonogramem (pominięte kopie zapasowe).

Alerty są generowane dla poszczególnych komputerów i wyświetlane na karcie **Alerty**.

Można określić liczbę dni bez kopii zapasowej, po których jest generowany alert.

Konsolidacja kopii zapasowych

Ta opcja określa, czy konsolidować kopie zapasowe podczas czyszczenia, czy też usuwać całe ciągi kopii zapasowych.

Ustawienie wstępne: **Wyłączone**.

Konsolidacja to proces polegający na połączeniu co najmniej dwóch kolejnych kopii zapasowych w jedną.

W przypadku włączenia tej opcji kopia zapasowa, która powinna zostać usunięta podczas czyszczenia, zostanie skonsolidowana z następną zależną kopią zapasową (przyrostową lub różnicową).

Jeśli opcja nie zostanie włączona, kopia zapasowa zostanie zachowana do czasu, gdy wszystkie zależne kopie zapasowe będą się kwalifikowały do usunięcia. Pomaga to uniknąć potencjalnie czasochłonnej konsolidacji, ale wymaga dodatkowego miejsca na przechowywanie kopii zapasowych, których usunięcie zostało opóźnione. Wiek bądź liczba kopii zapasowych może przekroczyć wartości określone w regułach przechowywania.

Ważne
Należy pamiętać, że konsolidacja to jedynie metoda usuwania, ale nie alternatywa dla usuwania. Wynikowa kopia zapasowa nie będzie zawierać danych, które były obecne w usuniętej kopii zapasowej i których nie było w zachowanej przyrostowej lub różnicowej kopii zapasowej.

Ta opcja *nie* jest skuteczna, jeśli występuje co najmniej jedna z następujących sytuacji:

- Miejscem docelowym kopii zapasowej jest magazyn chmurowy.
- Schemat tworzenia kopii zapasowych jest ustawiony jako **Zawsze przyrostowa (jednoplikowa)**.
- Format kopii zapasowej jest ustawiony jako **Wersja 12**.

© Acronis International GmbH, 2003-2024

Kopie zapasowe przechowywane w magazynie chmurowym oraz jednoplikowe kopie zapasowe w wersji 11 i 12 są zawsze konsolidowane, ponieważ ich struktura wewnętrzna umożliwia szybką i łatwą konsolidację.

Jednak w przypadku korzystania z wersji 12 oraz obecności wielu ciągów kopii zapasowych (każdy ciąg zapisywany w osobnym pliku .tibx) konsolidacja działa tylko w obrębie ostatniego ciągu. Wszystkie pozostałe ciągi są całkowicie usuwane – za wyjątkiem pierwszego, który jest pomniejszany do minimalnego rozmiaru pozwalającego na zachowanie metainformacji (około 12 KB). Te metainformacje są niezbędne do zapewnienia spójności danych podczas jednoczesnych operacji odczytu i zapisu. Zawarte w tych ciągach kopie zapasowe znikają z graficznego interfejsu użytkownika natychmiast po zastosowaniu reguły przechowywania, choć nadal istnieją fizycznie aż do usunięcia całego ciągu.

We wszystkich pozostałych przypadkach kopie zapasowe, których usunięcie zostanie wstrzymane, będą oznaczone w interfejsie graficznym ikoną kosza na śmieci ( ) Po usunięciu takiej kopii zapasowej poprzez kliknięcie symbolu X zostanie przeprowadzona konsolidacja.

Nazwa pliku kopii zapasowej

Ta opcja umożliwia zdefiniowanie nazw plików kopii zapasowych tworzonych przez plan ochrony lub plan tworzenia kopii zapasowych aplikacji w chmurze.

W przypadku plików kopii zapasowych tworzonych przez plany ochrony nazwy te są widoczne w menedżerze plików podczas przeglądania lokalizacji kopii zapasowych.

Co to jest plik kopii zapasowej?

W ramach każdego planu ochrony w lokalizacji kopii zapasowych jest tworzony co najmniej jeden plik — w zależności od używanego schematu tworzenia kopii zapasowych i formatu kopii zapasowych. Poniższa tabela zawiera pliki, które można utworzyć dla komputera lub skrzynki pocztowej.

	Zawsze przyrostowa (jednoplikowa)	**Inne schematy tworzenia kopii zapasowych**
Format kopii zapasowej **Wersja 11**	Jeden plik TIB i jeden plik metadanych XML	Wiele plików TIB i jeden plik metadanych XML
Format kopii zapasowej **Wersja 12**	Jeden plik TIBX na ciąg kopii zapasowych (pełna lub różnicowa kopia zapasowa oraz wszystkie przyrostowe kopie zapasowe, które od niej zależą). Jeśli rozmiar pliku przechowywanego w folderze lokalnym lub sieciowym (SMB) przekracza 200 GB, plik jest domyślnie dzielony na pliki o rozmiarze 200 GB.	

Wszystkie pliki mają taką samą nazwę z dodaną sygnaturą czasową lub numerem sekwencyjnym lub bez. Nazwę tę (określaną jako nazwa pliku kopii zapasowej) można zdefiniować podczas tworzenia lub edytowania planu ochrony lub planu tworzenia kopii zapasowych aplikacji w chmurze.

© Acronis International GmbH, 2003-2024

Uwaga
Sygnatura czasowa jest dodawana do nazwy pliku kopii zapasowej tylko w przypadku formatu w wersji 11.

W przypadku zmiany nazwy pliku kopii zapasowej w planie ochrony lub planie tworzenia kopii zapasowych aplikacji w chmurze kolejna kopia zapasowa będzie pełną kopią zapasową.

Jeśli podasz nazwę pliku już istniejącej kopii zapasowej danego komputera, zostanie utworzona pełna, przyrostowa lub różnicowa kopia zapasowa — zgodnie z harmonogramem planu.

Uwaga
Przenosząc pliki kopii zapasowych (.tibx) z ich pierwotnego magazynu nie zmieniaj ich nazw. Pliki ze zmienionymi nazwami będą wyglądać jak uszkodzone i nie będzie można odzyskać z nich danych.

Możesz ustawić nazwy plików kopii zapasowych na potrzeby lokalizacji, których nie można przeglądać za pomocą menedżera plików (np. chmury). W takim przypadku niestandardowe nazwy będą widoczne na karcie **Magazyn kopii zapasowych**.

Gdzie mogę zobaczyć nazwy plików kopii zapasowej?

W przypadku planów ochrony na karcie **Magazyn kopii zapasowych** wybierz lokalizację, a następnie archiwum kopii zapasowej.

- Domyślna nazwa pliku kopii zapasowej jest pokazywana na panelu **Szczegóły**.
- Jeśli ustawisz inną nazwę pliku kopii zapasowej niż domyślna, będzie ona bezpośrednio widoczna na karcie **Magazyn kopii zapasowych** w kolumnie **Nazwa**.

Jeśli chodzi o plany tworzenia kopii zapasowych aplikacji w chmurze, na karcie **Magazyn kopii zapasowych** wybierz lokalizację, wybierz archiwum kopii zapasowej, a następnie kliknij ikonę koła zębatego.

Ograniczenia nazw plików kopii zapasowej

- Nazwa pliku kopii zapasowej nie może kończyć się cyfrą.
  W domyślnej nazwie pliku kopii zapasowej, aby uniknąć kończenia nazwy cyfrą, dołączana jest litera „A”. Podczas tworzenia nazwy niestandardowej zawsze się upewnij, że nie kończy się ona cyfrą. W przypadku używania zmiennych nazwa pliku kopii zapasowej nie może się kończyć zmienną, ponieważ zmienna może kończyć się cyfrą.
- Nazwa pliku kopii zapasowej nie może zawierać następujących symboli: **()&?*$<>":\|/#**, znaków końca wiersza (**\n**) ani znaków tabulacji (**\t**).

Uwaga
Wybierz nazwy plików kopii zapasowych przyjazne dla użytkownika. Pozwoli to na łatwe rozróżnianie kopii zapasowych podczas przeglądania lokalizacji kopii zapasowych za pomocą menedżera plików.

© Acronis International GmbH, 2003-2024

Domyślna nazwa pliku kopii zapasowej

Domyślna nazwa pliku kopii zapasowej w przypadku kopii zapasowych całych komputerów fizycznych i maszyn wirtualnych, dysków/woluminów, plików/folderów, baz danych programu Microsoft SQL Server, baz danych programu Microsoft Exchange Server oraz konfiguracji ESXi to `[Machine Name]-[Plan ID]-[Unique ID]A`.

Domyślna nazwa kopii zapasowych skrzynek pocztowych programu Exchange i kopii zapasowych skrzynek pocztowych Microsoft 365 tworzonych przez lokalnego agenta dla usługi Microsoft 365 to `[Mailbox ID]_mailbox_[Plan ID]A`.

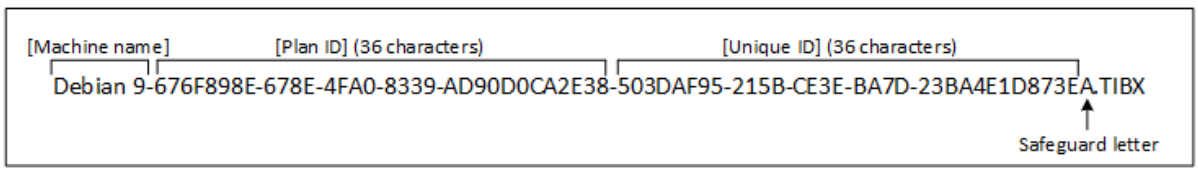
Domyślnie nazwy kopii zapasowych na platformie Microsoft Azure mają prefiks `[Mailbox ID]_`. Tego prefiksu nie można usunąć.

Domyślna nazwa kopii zapasowych aplikacji w chmurze tworzonych przez agentów w chmurze to `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`.

Domyślna nazwa zawiera następujące zmienne:

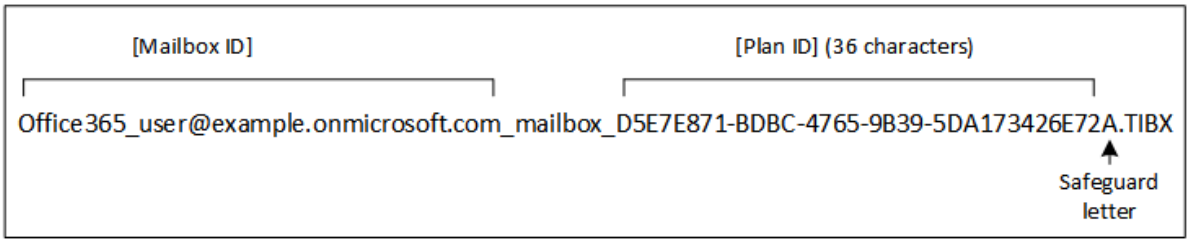
- `[Machine Name]` Ta zmienna jest zastępowana przez nazwę komputera lub maszyny wirtualnej (tę, która jest widoczna w konsoli Cyber Protect).
- `[Plan ID]`, `[Plan Id]` Ta zmienna jest zastępowana przez unikatowy identyfikator planu ochrony. Ta wartość się nie zmienia przy zmianie nazwy planu.
- `[Unique ID]` Ta zmienna jest zastępowana przez unikatowy identyfikator wybranego komputera lub maszyny wirtualnej. Ta wartość się nie zmienia przy zmianie nazwy komputera.
- `[Mailbox ID]` Ta zmienna jest zastępowana przez główną nazwę użytkownika skrzynki pocztowej.
- `[Resource Name]` Ta zmienna jest zastępowana przez nazwę chmurowego źródła danych, taką jak główna nazwa użytkownika skrzynki pocztowej, adres URL witryny SharePoint lub nazwa Dysku udostępnionego.
- `[Resource Type]` Ta zmienna jest zastępowana przez typ chmurowego źródła danych, taki jak `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive`.
- `[Resource ID]` Ta zmienna jest zastępowana przez unikatowy identyfikator chmurowego źródła danych. Ta wartość się nie zmienia przy zmianie nazwy chmurowego źródła danych.
- „`A`” to litera zabezpieczająca dołączana, aby uniknąć kończenia nazwy cyfrą.

Poniższy diagram pokazuje domyślną nazwę pliku kopii zapasowej.



Poniższy diagram przedstawia domyślną nazwę pliku kopii zapasowej skrzynek pocztowych Microsoft 365 utworzonej przez lokalnego agenta.

© Acronis International GmbH, 2003-2024



Nazwy bez zmiennych

Jeśli zmienisz nazwę pliku kopii zapasowej na `MyBackup`, pliki kopii zapasowej będą wyglądały podobnie do poniższych przykładów. Oba przykłady zakładają codzienne przyrostowe kopie zapasowe zaplanowane na 14:40, poczynając od 13 września 2016 r.

W przypadku formatu w wersji 12 ze schematem tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)**:

```
MyBackup.tibx
```

W przypadku formatu w wersji 12 z innymi schematami tworzenia kopii zapasowych:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Używanie zmiennych

Oprócz zmiennych, które są stosowane domyślnie, można używać następujących zmiennych:

- Zmienna `[Plan name]`, która jest zastępowana przez nazwę planu ochrony.
- Zmienna `[Virtualization Server Type]`, która jest zastępowana przez wartość „vmwesx”, jeśli kopie zapasowe maszyn wirtualnych są wykonywane przez agenta dla VMware, lub wartość „mshyperv”, jeśli kopie zapasowe maszyn wirtualnych są wykonywane przez agenta dla Hyper-V.

Jeśli do kopii zapasowej wybrano wiele komputerów lub skrzynek pocztowych, nazwa pliku kopii zapasowej musi zawierać zmienną `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]` lub `[Resource Id]`.

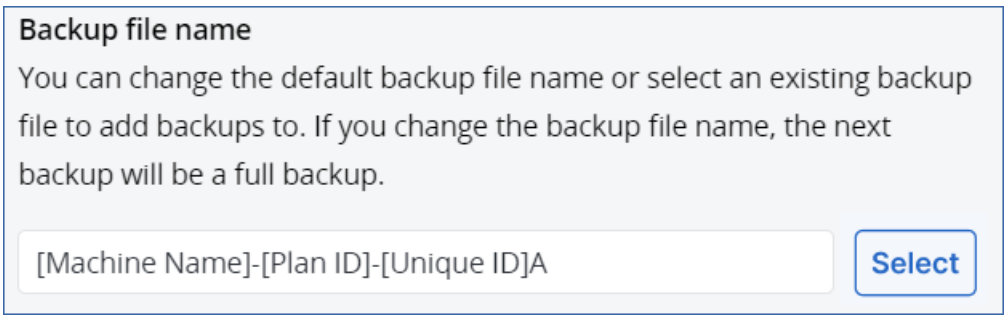
Tworzenie kopii zapasowych w już istniejącym archiwum kopii zapasowych

Można skonfigurować kopie zapasowe maszyny, które mają zostać dodane do już istniejącego archiwum kopii zapasowych.

Opcja ta może być przydatna na przykład wtedy, gdy plan ochrony jest zastosowany do jednego komputera i trzeba usunąć ten komputer z konsoli Cyber Protect lub odinstalować agenta wraz z jego ustawieniami konfiguracyjnymi. Po ponownym dodaniu komputera lub ponownej instalacji

© Acronis International GmbH, 2003-2024

agenta możesz wymusić w planie ochrony kontynuację tworzenia kopii zapasowych w oryginalnym archiwum.



Aby skonfigurować kopie zapasowe maszyny, które mają zostać dodane do już istniejącego archiwum kopii zapasowych

Obciążenia inne niż międzychmurowe

1. Na ekranie **Wszystkie urządzenia** kliknij maszynę, a następnie kliknij **Chroń**.
2. W ustawieniach planu ochrony rozszerz moduł **Kopia zapasowa**.
3. Kliknij **Opcje kopii zapasowych**, a następnie kliknij **Zmień**.
4. Na karcie **Nazwa pliku kopii zapasowej** kliknij **Wybierz**.
   Przycisk **Wybierz** pozwala wyświetlić kopie zapasowe w lokalizacji wybranej w sekcji **Miejsce docelowe kopii zapasowej** planu ochrony.

   Uwaga
   Przycisk **Wybierz** jest dostępny tylko w przypadku planów ochrony tworzonych i stosowanych na potrzeby jednego obciążenia.

5. Wybierz archiwum, a następnie kliknij **Gotowe**.
6. Kliknij **Gotowe**, a następnie **Zastosuj**.

Obciążenia międzychmurowe

1. Na karcie **Zarządzanie** > **Kopie zapasowe aplikacji w chmurze** wybierz plan.
2. Kliknij **Edytuj**, a następnie kliknij ikonę koła zębatego obok nazwy planu.
3. Na karcie **Nazwa pliku kopii zapasowej** kliknij **Wybierz**.

   Uwaga
   Przycisk **Wybierz** jest dostępny tylko w przypadku planów tworzenia kopii zapasowych utworzonych i zastosowanych do jednej maszyny.

4. Wybierz archiwum kopii zapasowych, a następnie kliknij **Gotowe**.
5. Kliknij **Gotowe**, a następnie kliknij **Zapisz zmiany**.

© Acronis International GmbH, 2003-2024

Format kopii zapasowej

Opcja **Format kopii zapasowej** określa format kopii zapasowych tworzonych w ramach danego planu ochrony. Opcja ta jest dostępna tylko w przypadku planów ochrony, w których jest już używany format kopii zapasowych w wersji 11. W takiej sytuacji można zmienić format kopii zapasowej na wersję 12. Po zmianie formatu kopii zapasowych na wersję 12 opcja ta przestanie być dostępna.

- **Wersja 11**

  Starszy format zachowany w celu zapewnienia kompatybilności wstecz.

  Uwaga
  Nie można tworzyć kopii zapasowych grup dostępności bazy danych (Database Availability Group, DAG) przy użyciu formatu kopii zapasowych w wersji 11. Tworzenie kopii zapasowych grup DAG jest obsługiwane tylko w formacie kopii zapasowych w wersji 12.

- **Wersja 12**

  Format kopii zapasowych, który został wprowadzony w programie Acronis Backup 12 w celu szybszego tworzenia kopii zapasowych i odzyskiwania. Każdy ciąg kopii zapasowych (pełna lub różnicowa kopia zapasowa oraz wszystkie przyrostowe kopie zapasowe, które od niej zależą) jest zapisywany w jednym pliku TIBX.

Format kopii zapasowej i pliki kopii zapasowej

W przypadku lokalizacji kopii zapasowej, które można przeglądać za pomocą menedżera plików (takich jak foldery lokalne lub sieciowe), format kopii zapasowej określa liczbę plików i ich rozszerzenia. Poniższa tabela zawiera pliki, które można utworzyć dla komputera lub skrzynki pocztowej.

	Zawsze przyrostowa (jednoplikowa)	**Inne schematy tworzenia kopii zapasowych**
Format kopii zapasowej **Wersja 11**	Jeden plik TIB i jeden plik metadanych XML	Wiele plików TIB i jeden plik metadanych XML
Format kopii zapasowej **Wersja 12**	Jeden plik TIBX na ciąg kopii zapasowych (pełna lub różnicowa kopia zapasowa oraz wszystkie przyrostowe kopie zapasowe, które od niej zależą). Jeśli rozmiar pliku przechowywanego w folderze lokalnym lub sieciowym (SMB) przekracza 200 GB, plik jest domyślnie dzielony na pliki o rozmiarze 200 GB.	

Zmienianie formatu kopii zapasowych na wersję 12 (TIBX)

Jeśli zmienisz format kopii zapasowych z wersji 11 (format TIB) na wersję 12 (format TIBX):

© Acronis International GmbH, 2003-2024

- Następna kopia zapasowa będzie pełna.
- W lokalizacjach kopii zapasowych, które można przeglądać za pomocą menedżera plików (takich jak foldery lokalne lub sieciowe), zostanie utworzony nowy plik TIBX. Nowy plik będzie mieć taką samą nazwę jak oryginalny plik oraz sufiks **_v12A**.
- Reguły przechowywania i replikacja będą stosowane tylko w przypadku nowych kopii zapasowych.
- Stare kopie zapasowe nie zostaną usunięte i nadal będą dostępne na karcie **Magazyn kopii zapasowych**.Można je usunąć ręcznie.
- Stare chmurowe kopie zapasowe nie będą wykorzystywać limitu **Chmura**.
- Stare lokalne kopie zapasowe będą wykorzystywać limit **Lokalna kopia zapasowa**, dopóki nie zostaną usunięte ręcznie.

Deduplikacja w archiwum

Format kopii zapasowych w wersji 12 — TIBX — obsługuje deduplikację w archiwum, co zapewnia następujące korzyści:

- Znacznie mniejszy rozmiar kopii zapasowych dzięki wbudowanej deduplikacji na poziomie bloków w przypadku każdego rodzaju danych
- Sprawna obsługa twardych łączy, która zapewnia wyeliminowanie duplikatów w magazynach
- Dzielenie na fragmenty na podstawie skrótów

Uwaga
Deduplikacja w archiwum jest domyślnie włączona w przypadku wszystkich kopii zapasowych w formacie TIBX. Nie trzeba jej włączać w opcjach tworzenia kopii zapasowych i nie można jej wyłączyć.

Kompatybilność formatów kopii zapasowych w różnych wersjach produktu

Informacje na temat kompatybilności formatów kopii zapasowych można znaleźć w sekcji Kompatybilność archiwów kopii zapasowych w różnych wersjach produktu (1689).

Sprawdzanie poprawności kopii zapasowej

Operacja sprawdzania poprawności polega na sprawdzeniu, czy można odzyskać dane z kopii zapasowej. W przypadku włączenia tej opcji każda kopia zapasowa utworzona w ramach planu ochrony jest od razu sprawdzana pod kątem poprawności metodą weryfikacji sumy kontrolnej. Ta operacja jest wykonywana przez agenta ochrony.

Ustawienie wstępne: **Wyłączono**.

Dodatkowe informacje na temat sprawdzania poprawności metodą weryfikacji sumy kontrolnej można znaleźć w sekcji "Weryfikacja sumy kontrolnej" (s. 238).

© Acronis International GmbH, 2003-2024

Uwaga
W zależności od ustawień wybranych przez dostawcę usług sprawdzanie poprawności może być niedostępne w przypadku tworzenia kopii zapasowej w chmurze. Sprawdzanie poprawności nie jest też dostępne w przypadku lokalizacji kopii zapasowych w chmurach publicznych.

CBT (Changed Block Tracking)

Ta opcja działa w przypadku następujących kopii zapasowych:

- Kopie zapasowe na poziomie dysku tworzone w przypadku maszyn wirtualnych
- Kopie zapasowe na poziomie dysku tworzone w przypadku komputerów fizycznych z systemem Windows
- Kopie zapasowe baz danych programu Microsoft SQL Server
- Kopie zapasowe baz danych programu Microsoft Exchange Server

Ustawienie wstępne: **Włączono**.

Ta opcja określa, czy podczas tworzenia przyrostowej lub różnicowej kopii zapasowej ma być używana funkcja Changed Block Tracking (CBT).

Technologia CBT przyspiesza proces tworzenia kopii zapasowych. Zmiany zawartości dysków lub baz danych są stale monitorowane na poziomie bloków. Po rozpoczęciu tworzenia kopii zapasowej zmiany mogą zostać niezwłocznie zapisane w kopii zapasowej.

Tryb tworzenia kopii zapasowych klastra

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Opcje te działają w przypadku kopii zapasowych na poziomie bazy danych programów Microsoft SQL Server i Microsoft Exchange Server.

Działają tylko wtedy, gdy do tworzenia kopii zapasowej został wybrany sam klaster [zawsze włączone grupy dostępności (AAG) programu Microsoft SQL Server lub grupa dostępności bazy danych (DAG) programu Microsoft Exchange Server], a nie poszczególne węzły lub znajdujące się w nich bazy danych. Jeśli wybierzesz poszczególne elementy wewnątrz klastra, kopia zapasowa nie będzie obsługiwać klastra i zostanie utworzona kopia zapasowa tylko wybranych kopii elementów.

Microsoft SQL Server

Ta opcja określa tryb kopii zapasowej dla zawsze włączonych grup dostępności (AAG) programu SQL Server. Aby ta opcja działała, agent dla SQL musi być zainstalowany na wszystkich węzłach zawsze włączonej grupy dostępności (AAG). Więcej informacji o tworzeniu kopii zapasowych zawsze włączonych grup dostępności, zobacz „Ochrona zawsze włączonych grup dostępności (AAG)”.

Ustawienie wstępne: **Replika pomocnicza, jeśli to możliwe.**

 © Acronis International GmbH, 2003-2024

Możesz wybrać jedną z poniższych opcji:

- **Replika pomocnicza, jeśli to możliwe**
  Jeśli wszystkie repliki pomocnicze są w trybie offline, jest tworzona kopia zapasowa repliki podstawowej. Tworzenie kopii zapasowej repliki podstawowej może spowolnić działanie programu SQL Server, ale kopia zapasowa zostanie utworzona dla najbardziej aktualnego stanu danych.
- **Replika pomocnicza**
  Jeśli wszystkie repliki pomocnicze są w trybie offline, operacja tworzenia kopii zapasowej się nie powiedzie. Tworzenie kopii zapasowych replik pomocniczych nie wpływa na wydajność SQL Server i umożliwia wydłużenie okna na utworzenie kopii zapasowej. Jednak pasywne repliki mogą zawierać nieaktualne informacje, ponieważ często są one aktualizowane asynchronicznie (z opóźnieniem).
- **Replika podstawowa**
  Jeśli replika podstawowa jest w trybie offline, operacja tworzenia kopii zapasowej się nie powiedzie. Tworzenie kopii zapasowej repliki podstawowej może spowolnić działanie programu SQL Server, ale kopia zapasowa zostanie utworzona dla najbardziej aktualnego stanu danych.

Bez względu na wartość tej opcji oprogramowanie, aby zapewnić spójność bazy danych, pomija bazy danych, które *nie* są w stanie **SYNCHRONIZED** lub **SYNCHRONIZING**, gdy rozpoczyna się tworzenie kopii zapasowej. Jeśli wszystkie bazy danych zostaną pominięte, operacja tworzenia kopii zapasowej się nie powiedzie.

Microsoft Exchange Server

Ta opcja określa tryb kopii zapasowej dla grup dostępności bazy danych (DAG) programu Exchange Server. Aby ta opcja działała, agent dla programu Exchange musi być zainstalowany na wszystkich węzłach grupy dostępności bazy danych (DAG). Więcej informacji o tworzeniu kopii zapasowych grup dostępności bazy danych, zobacz „Ochrona grup dostępności bazy danych (DAG)”.

Ustawienie wstępne: **Kopia pasywna, jeśli to możliwe.**

Możesz wybrać jedną z poniższych opcji:

- **Kopia pasywna, jeśli to możliwe**
  Jeśli wszystkie kopie pasywne są w trybie offline, jest tworzona kopia zapasowa kopii aktywnej. Tworzenie kopii zapasowej kopii aktywnej może spowolnić działanie programu Exchange Server, ale kopia zapasowa zostanie utworzona dla najbardziej aktualnego stanu danych.
- **Kopia pasywna**
  Jeśli wszystkie kopie pasywne są w trybie offline, operacja tworzenia kopii zapasowej się nie powiedzie. Tworzenie kopii zapasowych kopii pasywnych nie wpływa na wydajność serwera programu Exchange i umożliwia wydłużenie okna na utworzenie kopii zapasowej. Pasywne kopie mogą jednak zawierać nieaktualne informacje, ponieważ często są one aktualizowane asynchronicznie (z opóźnieniem).
- **Kopia aktywna**

© Acronis International GmbH, 2003-2024

Jeśli kopia aktywna jest w trybie offline, operacja tworzenia kopii zapasowej się nie powiedzie. Tworzenie kopii zapasowej kopii aktywnej może spowolnić działanie programu Exchange Server, ale kopia zapasowa zostanie utworzona dla najbardziej aktualnego stanu danych.

Bez względu na wartość tej opcji oprogramowanie, aby zapewnić spójność bazy danych, pomija bazy danych, które *nie* są w stanie **HEALTHY** lub **ACTIVE**, gdy rozpoczyna się tworzenie kopii zapasowej. Jeśli wszystkie bazy danych zostaną pominięte, operacja tworzenia kopii zapasowej się nie powiedzie.

Stopień kompresji

Uwaga
Ta opcja nie jest dostępna w przypadku tworzenia kopii zapasowych z chmury do chmury. W przypadku tych kopii zapasowych domyślnie jest włączona kompresja ze stałym poziomem odpowiadającym poziomowi **Normalny** poniżej.

Ta opcja określa stopień kompresji danych w tworzonej kopii zapasowej. Dostępne są następujące poziomy: **Brak**, **Normalny**, **Wysoki**, **Maksymalny**.

Ustawienie wstępne: **Normalny**.

Wyższy poziom kompresji powoduje, że utworzenie kopii zapasowej zabiera więcej czasu, ale wynikowa kopia zapasowa zajmuje mniej miejsca. Obecnie ustawienia poziomów **Wysoki** i **Maksymalny** działają podobnie.

Optymalny poziom kompresji danych zależy od typu danych uwzględnianych w kopii zapasowej. Nawet maksymalna kompresja nie wpłynie w sposób istotny na zmniejszenie rozmiaru kopii zapasowej, jeśli są w niej uwzględniane zasadniczo już skompresowane pliki, na przykład w formacie .jpg, .pdf lub .mp3. Jednak pliki w takich formatach jak .doc czy .xls zostaną dobrze skompresowane.

Obsługa błędów

Umożliwiają one określenie sposobu obsługi błędów, które mogą wystąpić podczas tworzenia kopii zapasowej.

W razie błędu spróbuj ponownie

Ustawienie wstępne: **Włączono. Liczba prób: 10. Odstęp między próbami: 30 s.**

Po wystąpieniu błędu, który można naprawić, program próbuje ponownie wykonać operację zakończoną niepowodzeniem. Można ustawić odstęp między kolejnymi próbami oraz ich liczbę. Ponowne próby zostaną wstrzymane po pomyślnym wykonaniu operacji lub wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

Jeśli na przykład lokalizacja docelowa kopii zapasowej w sieci będzie niedostępna lub nieosiągalna w czasie operacji tworzenia kopii zapasowej, oprogramowanie spróbuje nawiązać połączenie co 30 sekund, ale nie więcej niż 30 razy. Próby zostaną wstrzymane po wznowieniu połączenia lub po

© Acronis International GmbH, 2003-2024

wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

Jeśli jednak miejsce docelowe kopii zapasowej nie jest dostępne w momencie rozpoczęcia operacji tworzenia kopii zapasowej, zostanie podjętych tylko 10 prób.

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb cichy)

Ustawienie wstępne: **Włączono**.

Po włączeniu trybu dyskretnego program automatycznie obsługuje sytuacje wymagające działania użytkownika (poza obsługą uszkodzonych sektorów, która jest zdefiniowana jako osobna opcja). Jeśli operacja nie może być kontynuowana bez działania użytkownika, zakończy się niepowodzeniem. Szczegółowe informacje na temat operacji, w tym błędy, które wystąpiły, można znaleźć w dzienniku operacji.

Ignoruj uszkodzone sektory

Ustawienie wstępne: **Wyłączono**.

W przypadku wyłączenia tej opcji za każdym razem, gdy program napotka uszkodzony sektor, działaniu tworzenia kopii zapasowej zostanie przypisany status **Wymagane działanie**. Aby utworzyć kopię zapasową prawidłowych danych z dysku, któremu grozi nagła awaria, włącz ignorowanie uszkodzonych sektorów. Pozostałe dane zostaną uwzględnione w kopii zapasowej, a po zamontowaniu wynikowej kopii zapasowej dysku będzie można wyodrębnić prawidłowe pliki na innym dysku.

Uwaga
Pomijanie uszkodzonych sektorów nie jest obsługiwane w systemie Linux. Kopię zapasową systemu Linux z uszkodzonymi sektorami można utworzyć w trybie offline za pomocą generatora nośnika startowego w lokalnie zainstalowanej wersji programu Cyber Protect. W celu skorzystania z lokalnego generatora nośnika startowego trzeba mieć osobną licencję. Aby uzyskać pomoc, skontaktuj się z zespołem pomocy technicznej.

W razie błędu tworzenia migawki maszyny wirtualnej spróbuj ponownie

Ustawienie wstępne: **Włączono. Liczba prób: 3. Odstęp między próbami: 5 minut.**

W razie niepowodzenia wykonania migawki maszyny wirtualnej program ponownie próbuje wykonać operację, która zakończyła się niepowodzeniem. Można ustawić odstęp między kolejnymi próbami oraz ich liczbę. Ponowne próby zostaną wstrzymane po pomyślnym wykonaniu operacji LUB wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

© Acronis International GmbH, 2003-2024

Szybka przyrostowa/różnicowa kopia zapasowa

Jest ona dostępna podczas tworzenia przyrostowych i różnicowych kopii zapasowych na poziomie dysku.

Ta opcja nie działa (jest zawsze wyłączona) w przypadku woluminów sformatowanych w systemach plików JFS, ReiserFS3, ReiserFS4, ReFS lub XFS.

Ustawienie wstępne: **Włączono**.

W przyrostowej lub różnicowej kopii zapasowej są rejestrowane tylko zmiany danych. Aby przyspieszyć proces tworzenia kopii zapasowej, program ustala, czy plik się zmienił, na podstawie jego rozmiaru oraz daty/godziny jego ostatniej modyfikacji. Wyłączenie tej funkcji spowoduje, że program będzie porównywać całą zawartość plików z tymi przechowywanymi w kopii zapasowej.

Filtry plików (uwzględniające/wykluczające)

Za pomocą filtrów plików można uwzględnić w kopii zapasowej lub wykluczyć z niej tylko określone pliki i foldery.

Filtry plików są dostępne w przypadku tworzenia kopii zapasowych całego komputera oraz kopii zapasowych na poziomie dysku lub na poziomie plików, chyba że powiedziano inaczej.

Filtry plików nie są dostępne w systemach plików XFS, JFS, exFAT i ReiserFS4. Aby uzyskać więcej informacji, zobacz "Obsługiwane systemy plików" (s. 57).

Filtrów plików nie można stosować w przypadku dysków dynamicznych (woluminy LVM lub LDM) maszyn wirtualnych, których kopie zapasowe są wykonywane w trybie bezagentowym, na przykład za pomocą agenta dla VMware, agenta dla Hyper-V lub agenta dla Scale Computing.

Aby włączyć filtry plików

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. W sekcji **Opcje tworzenia kopii zapasowych** kliknij **Zmień**.
3. Wybierz **Filtry plików (wykluczające/uwzględniające)**.
4. Użyj dowolnych z niżej opisanych opcji.

Filtry uwzględniające i wykluczające

Istnieją dwa filtry: uwzględniające i wykluczające.

- **Uwzględnij tylko pliki spełniające następujące kryteria**
  Jeśli w filtrze uwzględniającym wpiszesz `C:\Plik.exe`, w kopii zapasowej zostanie uwzględniony tylko ten plik nawet wtedy, gdy wybierzesz opcję kopii zapasowej Cały komputer.

© Acronis International GmbH, 2003-2024

Uwaga
Ten filtr nie jest obsługiwany w przypadku kopii zapasowej na poziomie plików, jeśli ma ona format **Wersja 11**, a lokalizacją docelową kopii zapasowej nie jest chmura.

- **Wyklucz pliki spełniające następujące kryteria**
  Jeśli w filtrze wykluczającym wpiszesz `C:\Plik.exe`, plik ten zostanie pominięty podczas tworzenia kopii zapasowej nawet wtedy, gdy wybierzesz opcję kopii zapasowej Cały komputer.

Można używać obu filtrów naraz. Filtr wykluczający ma pierwszeństwo przed filtrem uwzględniającym, tj. w przypadku wpisania `C:\Plik.exe` w obu polach plik ten zostanie pominięty podczas tworzenia kopii zapasowej.

Kryteria filtrów

Jako kryteriów filtrów można używać nazw plików i folderów, pełnych ścieżek do plików i folderów oraz masek z symbolami wieloznacznymi.

W kryteriach filtrów nie jest rozróżniana wielkość liter. Na przykład w przypadku podania ścieżki `C:\Temp` zostaną też wybrane ścieżki `C:\TEMP` i `C:\temp`.

- Nazwa
  Określ nazwę pliku lub folderu, na przykład `Dokument.txt`. Zostaną wybrane wszystkie pliki i foldery o tej nazwie.
- Pełna ścieżka
  Określ pełną ścieżkę do pliku lub folderu, zaczynając od litery dysku (w przypadku tworzenia kopii zapasowych danych systemu Windows) lub katalogu głównego (w przypadku tworzenia kopii zapasowych systemu Linux lub macOS). W systemach Windows, Linux i macOS można używać ukośników (np. `C:/Temp/Plik.tmp`). W systemie Windows można też używać tradycyjnych ukośników odwrotnych (np. `C:\Temp\Plik.tmp`).

  Ważne
  Jeśli podczas tworzenia kopii zapasowej na poziomie dysku system operacyjny uwzględnianego w kopii komputera nie zostanie poprawnie wykryty, filtry plików oparte na pełnych ścieżkach nie będą działać. W przypadku filtru wykluczającego pojawi się ostrzeżenie. W przypadku filtru uwzględniającego operacja tworzenia kopii zapasowej się nie powiedzie.
  Na przykład pełna ścieżka do pliku może wyglądać następująco: `C:\Temp\Plik.tmp`. Filtr w postaci pełnej ścieżki, obejmującej literę dysku lub katalog główny, na przykład `C:\Temp\Plik.tmp` lub `C:\Temp\*`, spowoduje wygenerowanie ostrzeżenia lub niepowodzenie operacji.
  Filtr, który nie obejmuje litery dysku lub katalogu głównego (na przykład `Temp\*` lub `Temp\Plik.tmp`) lub filtr zaczynający się gwiazdką (na przykład `*C:\`) nie spowoduje wygenerowania ostrzeżenia ani niepowodzenia operacji. Jeśli jednak system operacyjny komputera uwzględnianego w kopii zapasowej nie zostanie poprawnie wykryty, te filtry plików również nie będą działać.

- Maska

© Acronis International GmbH, 2003-2024

W przypadku nazw i pełnych ścieżek można używać następujących symboli wieloznacznych: gwiazdka (*), dwie gwiazdki (**) i znak zapytania (?).

Gwiazdka (*) reprezentuje zero lub więcej znaków. Na przykład do kryterium filtru **Dok*.txt** pasuje plik `Dok.txt` i plik `Dokument.txt`.

Dwie gwiazdki (**) reprezentują zero lub więcej znaków, w tym znak ukośnika. Na przykład do kryterium ****/Dokumenty/**.txt** pasują wszystkie pliki TXT we wszystkich podfolderach wszystkich folderów o nazwie `Dokumenty`. Dwóch gwiazdek (**) można używać tylko w przypadku kopii zapasowych w formacie Wersja 12.

Znak zapytania (?) reprezentuje tylko jeden znak. Na przykład do kryterium **Dok?.txt** pasują takie pliki jak `Dok1.txt` i `DokB.txt`, ale nie pliki `Dok.txt` czy `Dok11.txt`.

Migawka kopii zapasowej na poziomie plików

Ta opcja jest dostępna tylko w przypadku kopii zapasowej na poziomie plików.

Ta opcja określa, czy kopia zapasowa ma być tworzona kolejno dla poszczególnych plików, czy też jako szybka migawka.

Uwaga
Pliki przechowywane w udziałach sieciowych zawsze są pojedynczo dodawane do kopii zapasowej.

Ustawienie wstępne:

- Jeśli do uwzględnienia w kopii zapasowej wybrano tylko komputery z systemem Linux: **Nie twórz migawki.**
- W przeciwnym razie: **Utwórz migawkę, jeśli to możliwe.**

Można wybrać jedną z następujących opcji:

- **Utwórz migawkę, jeśli to możliwe**
  Jeśli nie można wykonać migawki, należy utworzyć bezpośrednią kopię zapasową plików.
- **Zawsze twórz migawkę**
  Migawka pozwala na utworzenie kopii zapasowej wszystkich plików, w tym plików, do których dostęp jest ograniczony. W kopii zapasowej zostaną uwzględnione pliki z tego samego punktu w czasie. Wybierz to ustawienie tylko wtedy, gdy są to krytyczne kwestie, tj. gdy nie ma sensu tworzyć kopii zapasowej plików bez migawki. Jeśli nie można utworzyć migawki, utworzenie kopii zapasowej zakończy się niepowodzeniem.
- **Nie twórz migawki**
  Zawsze wykonuj bezpośrednią kopię zapasową plików. Próba utworzenia kopii zapasowej plików otwartych do wyłącznego dostępu zakończy się błędem odczytu. Pliki w kopii zapasowej mogą być niespójne czasowo.

Dane do analizy śledczej

Wirusy, złośliwe oprogramowanie i oprogramowanie ransomware mogą wykonywać szkodliwe działania, takie jak kradzież czy zmienianie danych. Działania tego typu mogą wymagać prac

© Acronis International GmbH, 2003-2024

dochodzeniowych, ale są one możliwe tylko wtedy, gdy na komputerze są przechowywane dowody cyfrowe. Jednak niektóre dowody cyfrowe, takie jak pliki czy ślady aktywności, mogą zostać usunięte lub komputer, na którym doszło do szkodliwych działań, może przestać być dostępny.

Kopie zapasowe z danymi do analizy śledczej pozwolą prowadzącym dochodzenie na analizę tych obszarów dysku, które zazwyczaj nie są uwzględniane w zwykłej kopii zapasowej. Opcja tworzenia kopii zapasowej **Dane do analizy śledczej** umożliwia zbieranie dowodów cyfrowych, które można wykorzystać w dochodzeniach śledczych: migawek nieużywanego miejsca na dysku, zrzutów pamięci i migawek uruchomionych procesów.

Kopie zapasowe na potrzeby analizy śledczej są automatycznie notaryzowane.

Opcja **Dane do analizy śledczej** jest dostępna tylko w przypadku kopii zapasowych całych komputerów z systemem Windows w następujących wersjach:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 — Windows Server 2019

Tworzenie kopii zapasowych z danymi do analizy śledczej nie jest obsługiwane w przypadku następujących komputerów:

- Komputery, które mają połączenie VPN z siecią, a nie mają bezpośredniego dostępu do Internetu
- Komputery z dyskami zaszyfrowanymi przy użyciu funkcji BitLocker

Uwaga
Po zastosowaniu do komputera planu ochrony z włączonym modułem **Kopia zapasowa** nie można zmieniać ustawień danych do analizy śledczej. Jeśli zechcesz użyć innych ustawień takich danych, utwórz nowy plan ochrony.

Kopie zapasowe z danymi do analizy śledczej można przechowywać w następujących lokalizacjach:

- Chmura
- Folder lokalny

  Uwaga
  Folder lokalny jest obsługiwany tylko na zewnętrznym dysku twardym podłączonym przez port USB.
  Lokalne dyski dynamiczne nie są obsługiwane jako lokalizacja kopii zapasowych z danymi do analizy śledczej.

- Folder sieciowy

Proces tworzenia kopii zapasowej na potrzeby analizy śledczej

Podczas tworzenia kopii zapasowej na potrzeby analizy śledczej system wykonuje następujące czynności:

© Acronis International GmbH, 2003-2024

1. Zapisuje surowy zrzut pamięci i listę uruchomionych procesów.
2. Automatycznie uruchamia ponownie komputer przy użyciu nośnika startowego.
3. Tworzy kopię zapasową, która zawiera zarówno zajmowane, jak i niealokowane miejsce.
4. Notaryzuje dyski uwzględniane w kopii zapasowej.
5. Uruchamia się ponownie w trybie systemu operacyjnego na żywo i kontynuuje wykonywanie planu (np. replikację, przechowywanie, sprawdzenie poprawności i inne).

Aby skonfigurować zbieranie danych do analizy śledczej

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**. Plan ochrony można też utworzyć na karcie **Zarządzanie**.
2. Wybierz urządzenie i kliknij **Chroń**.
3. W planie ochrony w ustawieniach modułu Kopia zapasowa włącz moduł **Kopia zapasowa**.
4. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Cały komputer**.
5. W sekcji **Opcje tworzenia kopii zapasowych** kliknij **Zmień**.
6. Znajdź opcję **Dane do analizy śledczej**.
7. Włącz **Zbierz dane do analizy śledczej**. System automatycznie pobierze zrzut pamięci i utworzy migawkę uruchomionych procesów.

   Uwaga
   Pełny zrzut pamięci może zawierać poufne dane, na przykład hasła.

8. Podaj lokalizację.
9. Kliknij **Uruchom teraz**, aby niezwłocznie utworzyć kopię zapasową z danymi do analizy śledczej, lub poczekaj na utworzenie kopii zapasowej zgodnie z harmonogramem.
10. Przejdź do sekcji **Monitorowanie** > **Działania** i sprawdź, czy kopia zapasowa z danymi do analizy śledczej została pomyślnie utworzona.

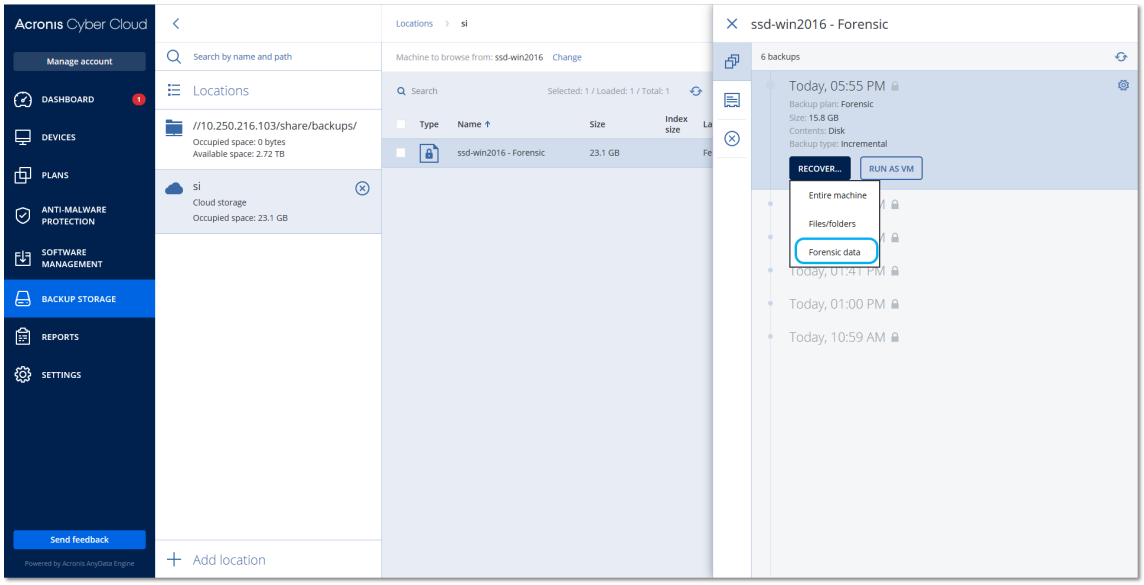
W wyniku tych działań kopie zapasowe będą zawierały dane do analizy śledczej, które będzie można pobrać i przeanalizować. Kopie zapasowe z danymi do analizy śledczej są oznaczone i można je wyfiltrować spośród innych kopii zapasowych w sekcji **Magazyn kopii zapasowych** > **Lokalizacje** za pomocą opcji **Tylko z danymi do analizy śledczej**.

Jak pobrać dane do analizy śledczej z kopii zapasowej?

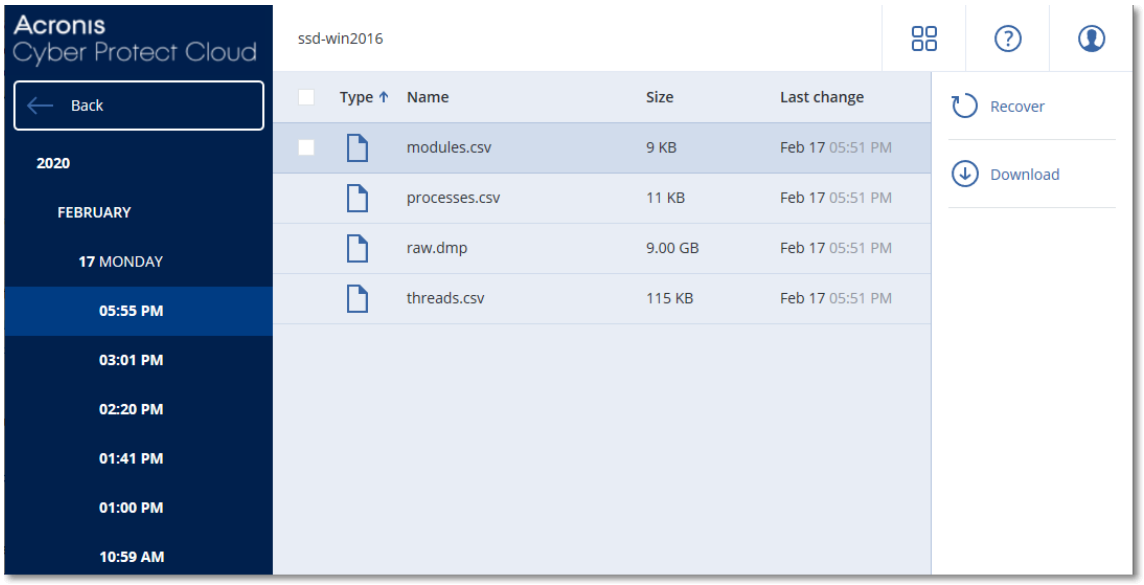
1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych** i wybierz lokalizację z kopiami zapasowymi zawierającymi dane do analizy śledczej.
2. Zaznacz odpowiednią kopię zapasową z danymi do analizy śledczej i kliknij **Pokaż kopie zapasowe**.
3. Kliknij **Odzyskaj** w wierszu właściwej kopii zapasowej.

© Acronis International GmbH, 2003-2024

- Aby odzyskać tylko dane do analizy śledczej, kliknij **Dane do analizy śledczej**.



System wyświetli folder z danymi do analizy śledczej. Wybierz plik zrzutu pamięci lub dowolny inny plik przeznaczony do analizy śledczej, a następnie kliknij **Pobierz**.



- Aby odzyskać całą kopię zapasową z danymi do analizy śledczej, kliknij **Cały komputer**. System odzyska kopię zapasową bez trybu startowego. Dzięki temu będzie można sprawdzić, czy dysk nie został zmieniony.

Dostępny zrzut pamięci można poddać dogłębniejszym analizom za pomocą kilku programów do analizy śledczej innych firm, na przykład programu Volatility Framework: https://www.volatilityfoundation.org/.

Notaryzacje kopii zapasowych z danymi do analizy śledczej

Aby umożliwić sprawdzenie, czy kopia zapasowa z danymi do analizy śledczej jest dokładnie tym samym obrazem, który został utworzony, tj. że nie został naruszony, moduł kopii zapasowej dokonuje notaryzacji kopii zapasowych z danymi do analizy śledczej.

© Acronis International GmbH, 2003-2024

Sposób działania

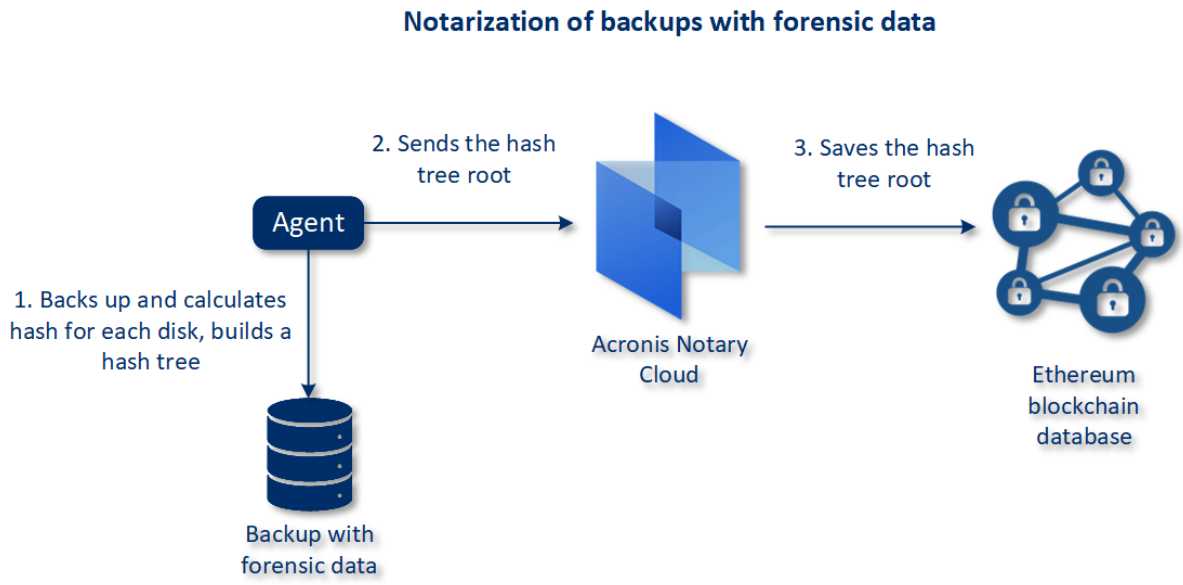
Notaryzacja pozwala udowodnić, że dysk z danymi do analizy śledczej jest autentyczny i niezmieniony od chwili uwzględnienia w kopii zapasowej.

Podczas tworzenia kopii zapasowej agent oblicza kody skrótów uwzględnianych w kopii dysków, buduje drzewo skrótów, zapisuje drzewo w kopii zapasowej, a następnie wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji zapisuje główne drzewo skrótów w bazie danych łańcucha bloków Ethereum, aby zapewnić, że ta wartość nie zostanie zmieniona.

Weryfikując autentyczność dysku z danymi do analizy śledczej, agent oblicza jego skrót, a następnie porównuje go ze skrótem przechowywanym w drzewie skrótów w kopii zapasowej. W przypadku niezgodności skrótów uznaje się, że dysk nie jest autentyczny. W przeciwnym razie autentyczność dysku jest gwarantowana przez drzewo skrótów.

Aby zweryfikować, czy samo drzewo skrótów nie zostało naruszone, agent wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji porównuje je z drzewem przechowywanym w bazie danych łańcucha bloków. Jeśli skróty są zgodne, wybrany dysk na pewno jest autentyczny. W przeciwnym razie program wyświetla komunikat, że dysk nie jest autentyczny.

Poniższy schemat obrazuje w skrócie proces notaryzacji kopii zapasowych z danymi do analizy śledczej.



Aby ręcznie zweryfikować notaryzowaną kopię zapasową dysku, można uzyskać dla niej certyfikat i postąpić zgodnie z wyświetlaną procedurą weryfikacji przy użyciu certyfikatu, korzystając z narzędzia tibxread.

Uzyskiwanie certyfikatu na potrzeby kopii zapasowych z danymi do analizy śledczej

Aby uzyskać z konsoli certyfikat na potrzeby kopii zapasowej z danymi do analizy śledczej:

© Acronis International GmbH, 2003-2024

1. Przejdź do sekcji **Magazyn kopii zapasowych** i zaznacz kopię zapasową z danymi do analizy śledczej.
2. Odzyskaj cały komputer.
3. System otworzy się w widoku **Mapowanie dysków**.
4. Kliknij ikonę **Uzyskaj certyfikat** w wierszu dysku.
5. System wygeneruje certyfikat i otworzy go w nowym oknie przeglądarki. Pod certyfikatem będzie dostępna instrukcja ręcznej weryfikacji notaryzowanej kopii zapasowej dysku.

Narzędzie „tibxread" do pobierania danych z kopii zapasowej

Cyber Protection udostępnia narzędzie `tibxread`, które umożliwia ręczne sprawdzenie integralności dysku z kopii zapasowej. Narzędzie to pozwala na pobranie danych z kopii zapasowej i obliczenie skrótu wybranego dysku. Jest ono instalowane automatycznie wraz z następującymi komponentami: agent dla systemu Windows, agent dla systemu Linux i agent dla system Mac.

Ścieżka instalacji: ten sam folder, w którym znajduje się agent (na przykład `C:\Program Files\BackupClient\BackupAndRecovery`).

Obsługiwane lokalizacje:

- Dysk lokalny
- Folder sieciowy (CIFS/SMB), który jest dostępny bez wymaganych poświadczeń.
  W przypadku folderu sieciowego chronionego hasłem można za pomocą narzędzi systemu operacyjnego zamontować folder sieciowy do folderu lokalnego, a następnie użyć tego folderu lokalnego jako źródła dla narzędzia.
- Chmura
  Należy podać adres URL, port i certyfikat. Adres URL i port można uzyskać z klucza rejestru systemu Windows lub plików konfiguracyjnych na komputerach z systemem Linux/Mac.
  W przypadku systemu Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<nazwa_logowania_dzierżawcy>\FesUri
  ```

  W przypadku systemu Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  W przypadku systemu macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  Certyfikat można znaleźć w następujących lokalizacjach:
  W przypadku systemu Windows:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```


© Acronis International GmbH, 2003-2024

W przypadku systemu Linux:

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

W przypadku systemu macOS:

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

Narzędzie obsługuje następujące polecenia:

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

Umożliwia wyświetlenie listy punktów odzyskiwania dostępnych w kopii zapasowej.

SKŁADNIA:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Opcje

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

Wzór danych wyjściowych:

```
GUID   Data   Sygnatura daty
----   ------ --------------
<guid> <data> <sygnatura daty>
```

<guid> — identyfikator GUID kopii zapasowej.

<date> — data utworzenia kopii zapasowej. Stosowany format daty to „DD.MM.RRRR GG24:MM:SS”. Domyślnie w lokalnej strefie czasowej (można ją zmienić za pomocą opcji --utc).

Przykład danych wyjściowych:

```
GUID   Data   Sygnatura daty
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```


© Acronis International GmbH, 2003-2024

list content

Umożliwia wyświetlenie listy zawartości punktu odzyskiwania.

SKŁADNIA:

```
tibxread list content --loc=URI --arc=NAZWA_KOPII_ZAPASOWEJ --password --backup=ID_
PUNKTU_ODZYSTKIWANIA --raw --log=ŚCIEŻKA
```

Opcje

```
--loc=URI
--arc=NAZWA_KOPII_ZAPASOWEJ
--password
--backup=ID_PUNKTU_ODZYSKIWANIA
--raw
--log=ŚCIEŻKA
```

Wzór danych wyjściowych:

```
Dysk     Rozmiar   Status notaryzacji
-------- ------ ---------------------
<nr> <rozmiar> <status_notaryzacji>
```

<number> — identyfikator dysku.

<size> — rozmiar w bajtach.

<notarization_status> — możliwe są następujące statusy: Bez notaryzacji, Notaryzowano, Następna kopia zapasowa.

Przykład danych wyjściowych:

```
Dysk     Rozmiar   Status notaryzacji
-------- ------ --------------
1        123123465798 Notaryzowano
2        123123465798 Notaryzowano
```

get content

Umożliwia zapisanie zawartości wskazanego dysku w punkcie odzyskiwania na standardowym wyjściu danych (stdout).

SKŁADNIA:

```
tibxread get content --loc=URI --arc=NAZWA_KOPII_ZAPASOWEJ --password --backup=ID_
PUNKTU_ODZYSKIWANIA --disk=NUMER_DYSKU --raw --log=ŚCIEŻKA --progress
```

Opcje

© Acronis International GmbH, 2003-2024

```
--loc=URI
--arc=NAZWA_KOPII_ZAPASOWEJ
--password
--backup=ID_PUNKTU_ODZYSKIWANIA
--disk=NUMER_DYSKU
--raw
--log=ŚCIEŻKA
--progress
```

calculate hash

Umożliwia obliczenie skrótu wskazanego dysku w punkcie odzyskiwania za pomocą algorytmu SHA-2 (256-bitowego) i zapisanie go na wyjściu stdout.

SKŁADNIA:

```
tibxread calculate hash --loc=URI --arc=NAZWA_KOPII_ZAPASOWEJ --password --backup=ID_
PUNKTU_ODZYSKIWANIA --disk=NUMER_DYSKU --raw --log=ŚCIEŻKA --progress
```

Opcje

```
--loc=URI
--arc=NAZWA_KOPII_ZAPASOWEJ
--password
--backup=ID_PUNKTU_ODZYSKIWANIA
--disk=NUMER_DYSKU
--raw
--log=ŚCIEŻKA
```

Opis opcji

Opcja	Opis
--arc=NAZWA_KOPII_ZAPASOWEJ	Nazwę pliku kopii zapasowej można znaleźć we właściwościach kopii zapasowej w konsoli Cyber Protect. Nazwę pliku kopii zapasowej należy podać wraz z rozszerzeniem .tibx.
--backup=IDENTYFIKATOR_PUNKTU_ODZYSKIWANIA	Identyfikator punktu odzyskiwania.
--disk=NUMER_DYSKU	Numer dysku (ten sam, który został zapisany w danych wyjściowych polecenia „get content”).
--loc=IDENTYFIKATOR_URI	Identyfikator URI lokalizacji kopii zapasowej. Możliwe formaty opcji „--loc”: • Nazwa ścieżki lokalnej (Windows) `c:/upload/backups` • Nazwa ścieżki lokalnej (Linux)

© Acronis International GmbH, 2003-2024

	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Chmura
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	`<IP_address>` — można go znaleźć w kluczu rejestru w systemie Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<nazwa_logowania_dzierżawcy>\FesUri
	`<path_to_certificate>` — ścieżka do pliku certyfikatu używanego w celu uzyskania dostępu do platformy Cyber Protect Cloud. Na przykład w systemie Windows certyfikat można znaleźć w folderze `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<nazwa_użytkownika>.crt`, gdzie <nazwa_użytkownika> jest nazwą konta używanego w celu uzyskania dostępu do platformy Cyber Protect Cloud.

--log=PATH	Aktywuje zapisywanie dzienników w określonej ŚCIEŻCE (tylko ścieżka lokalna, format jest taki sam jak w przypadku parametru `--loc=URI`). Stosowany jest poziom dziennika DEBUG.
--password=PASSWORD	Hasło szyfrowania kopii zapasowej. Jeśli kopia zapasowa nie jest zaszyfrowana, pozostaw tę wartość pustą.

--raw	Umożliwia ukrycie nagłówków (dwóch pierwszych wierszy) w danych wyjściowych polecenia. Jest używany w sytuacji, gdy powinny być analizowane dane wyjściowe polecenia.
	Przykład danych wyjściowych bez parametru „`--raw`”:
	`GUID Data Sygnatura daty`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Dane wyjściowe z parametrem „`--raw`”:
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	Umożliwia wyświetlenie dat w standardzie UTC.

--progress	Umożliwia wyświetlenie postępu operacji.
	Na przykład:
	`1%`
	`2%`
	`3%`
	`4%`

© Acronis International GmbH, 2003-2024

	``` ... 100% ```

Obcinanie dziennika

Ta opcja jest dostępna w przypadku tworzenia kopii zapasowej baz danych programu Microsoft SQL Server oraz kopii zapasowej na poziomie dysku przy włączonym tworzeniu kopii zapasowej aplikacji Microsoft SQL Server.

Opcja umożliwia określenie, czy po pomyślnym utworzeniu kopii zapasowej mają być obcinane dzienniki transakcji programu SQL Server.

Ustawienie wstępne: **Włączono**.

W przypadku włączenia tej opcji bazę danych można odzyskać tylko do punktu w czasie kopii zapasowej utworzonej przez oprogramowanie. Tworząc kopię zapasową dzienników transakcji za pomocą macierzystego aparatu tworzenia kopii zapasowych programu Microsoft SQL Server, opcję tę należy wyłączyć. Po odzyskaniu można zastosować dzienniki transakcji i dzięki temu odzyskać bazę danych do dowolnego punktu w czasie.

Wykonywanie migawek LVM

Ta opcja jest dostępna tylko w przypadku komputerów fizycznych.

Opcja jest dostępna w przypadku tworzenia kopii zapasowej na poziomie dysku uwzględniającej woluminy zarządzane przez narzędzie Logical Volume Manager (LVM) systemu Linux. Woluminy takie określa się także mianem woluminów logicznych.

Ta opcja określa sposób wykonywania migawki woluminu logicznego. Program do tworzenia kopii zapasowych może wykonywać tę operację samodzielnie lub przy użyciu narzędzia Logical Volume Manager (LVM) systemu Linux.

Ustawienie wstępne: **Za pomocą oprogramowania do tworzenia kopii zapasowych**.

- **Za pomocą oprogramowania do tworzenia kopii zapasowych**. Dane migawki są przechowywane głównie w pamięci RAM. Dzięki temu kopie zapasowe są tworzone szybciej i nie jest potrzebne nieprzydzielone miejsce w grupie woluminów. Dlatego zaleca się zmianę ustawienia wstępnego tylko w przypadku problemów z tworzeniem kopii zapasowych woluminów logicznych.
- **Za pomocą menedżera LVM**. Migawka jest zapisywana w nieprzydzielonym miejscu w grupie woluminów. Jeśli nie ma nieprzydzielonego miejsca, migawka zostanie wykonana przez oprogramowanie do tworzenia kopii zapasowych.

Migawka jest używana tylko podczas operacji tworzenia kopii zapasowej i jest automatycznie usuwana po zakończeniu tej operacji. Nie są przechowywane żadne pliki tymczasowe.

© Acronis International GmbH, 2003-2024

Punkty zamontowania

Ta opcja jest dostępna tylko w systemie Windows na potrzeby tworzenia kopii zapasowych na poziomie plików uwzględniającej źródło danych obejmujące zamontowane woluminy lub udostępnione woluminy klastra.

Ta opcja jest dostępna tylko w przypadku, gdy folder wybrany do utworzenia kopii zapasowej znajduje się wyżej w hierarchii folderów niż punkt zamontowania. (punkt zamontowania to folder, do którego został logicznie podłączony dodatkowy wolumin).

- W przypadku wybrania takiego folderu (folderu nadrzędnego) do uwzględnienia w kopii zapasowej i włączenia opcji **Punkty zamontowania** w kopii zapasowej zostaną uwzględnione wszystkie pliki znajdujące się w zamontowanym woluminie. Jeśli opcja **Punkty zamontowania** będzie wyłączona, punkt zamontowania w kopii zapasowej będzie pusty.

  Odzyskanie zawartości punktu zamontowania podczas odzyskiwania folderu nadrzędnego zależy od włączenia lub wyłączenia opcji **Punkty zamontowania** w ramach operacji odzyskiwania.
- Jeśli wybierzesz punkt zamontowania bezpośrednio lub wybierzesz dowolny folder na woluminie zamontowania, wybrane foldery będą traktowane jak foldery zwykłe. Zostaną uwzględnione w kopii zapasowej niezależnie od stanu opcji **Punkty zamontowania** i odzyskane bez względu na stan opcji **Punkty zamontowania** w ramach operacji odzyskiwania.

Ustawienie wstępne: **Wyłączono**.

Uwaga
Można tworzyć kopie zapasowe maszyn wirtualnych Hyper-V znajdujących się na udostępnionym woluminie klastra, uwzględniając w niej wymagane pliki lub cały wolumin w ramach tworzenia kopii zapasowej na poziomie plików. Należy tylko pamiętać o wyłączeniu maszyn wirtualnych, aby ich kopia zapasowa była spójna.

Przykład

Załóżmy, że folder **C:\Dane1** jest punktem zamontowania woluminu. Wolumin zawiera foldery **Folder1** i **Folder2**. Tworzysz plan ochrony na potrzeby kopii zapasowej danych na poziomie plików.

Jeśli zaznaczysz pole wyboru woluminu C i włączysz opcję **Punkty zamontowania**, folder **C:\Dane1** w kopii zapasowej będzie zawierać foldery **Folder1** i **Folder2**. W przypadku odzyskiwania danych z kopii zapasowej należy pamiętać o poprawnym zastosowaniu opcji **Punkty zamontowania** w ramach operacji odzyskiwania.

Jeśli zaznaczysz pole wyboru woluminu C i wyłączysz opcję **Punkty zamontowania**, folder **C:\Dane1** w kopii zapasowej będzie pusty.

Jeśli zaznaczysz pole wyboru folderu **Dane1**, folder **Folder1** lub **Folder2**, zaznaczone foldery zostaną uwzględnione w kopii zapasowej jako zwykłe foldery bez względu na stan opcji **Punkty zamontowania**.

© Acronis International GmbH, 2003-2024

Migawka wielowoluminowa

Ta opcja jest dostępna w przypadku kopii zapasowych komputerów fizycznych z systemem Windows lub Linux.

Opcja ta dotyczy kopii zapasowej na poziomie dysku. Opcja ta dotyczy również kopii zapasowej na poziomie plików, jeśli kopia zapasowa jest tworzona przez wykonanie migawki (opcja Migawka kopii zapasowej na poziomie plików określa, czy podczas tworzenia kopii zapasowej na poziomie plików jest wykonywana migawka).

Ta opcja określa, czy migawki kilku woluminów mają zostać utworzone jednocześnie, czy po kolei.

Ustawienie wstępne:

- Jeśli do uwzględnienia w kopii zapasowej wybrano co najmniej jeden komputer z systemem Windows: **Włączono**.
- W przeciwnym razie: **Wyłączono**.

W przypadku włączenia tej opcji migawki wszystkich woluminów uwzględnianych w kopii zapasowej są tworzone jednocześnie. Użyj tej opcji, aby utworzyć spójną czasowo kopię zapasową danych na wielu woluminach, na przykład dla bazy danych Oracle.

Jeśli ta opcja jest wyłączona, migawki woluminów są wykonywane po kolei. W rezultacie utworzona w ten sposób kopia zapasowa może nie być spójna, jeśli dane znajdują się na wielu woluminach.

Odzyskiwanie jednym kliknięciem

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Dzięki funkcji Odzyskiwanie jednym kliknięciem możesz automatycznie odzyskać kopię zapasową dysku komputera z systemem Windows lub Linux. Ta kopia zapasowa może być kopią zapasową całego komputera albo kopią zapasową określonych dysków lub woluminów na tym komputerze.

Funkcja Odzyskiwanie jednym kliknięciem obsługuje następujące operacje:

- Automatyczne odzyskiwanie z ostatniej kopii zapasowej
- Odzyskiwanie z określonej kopii zapasowej (nazywanej również punktem odzyskiwania) dostępnej w archiwum kopii zapasowych

Funkcja Odzyskiwanie jednym kliknięciem obsługuje następujące magazyny kopii zapasowych:

- Secure Zone
- Folder lokalny
- Folder sieciowy
- Chmura

© Acronis International GmbH, 2003-2024

Ważne
W przypadku wykonywania jednej z następujących operacji wstrzymaj szyfrowanie funkcją BitLocker do następnego ponownego uruchomienia komputera:

- Tworzenie, modyfikowanie lub usuwanie partycji Secure Zone.
- Włączanie lub wyłączanie programu Startup Recovery Manager.
- [Tylko w przypadku, gdy program Startup Recovery Manager nie był jeszcze włączony] Uruchamianie pierwszej kopii zapasowej po włączeniu odzyskiwania jednym kliknięciem w planie ochrony. Ta operacja powoduje automatyczne włączenie programu Startup Recovery Manager.
- Aktualizowanie programu Startup Recovery Manager, na przykład poprzez aktualizowanie ochrony.

Jeśli szyfrowanie funkcją BitLocker nie zostało wstrzymane podczas tych operacji, po ponownym uruchomieniu komputera konieczne będzie podanie kodu PIN funkcji BitLocker.

Włączanie funkcji Odzyskiwanie jednym kliknięciem

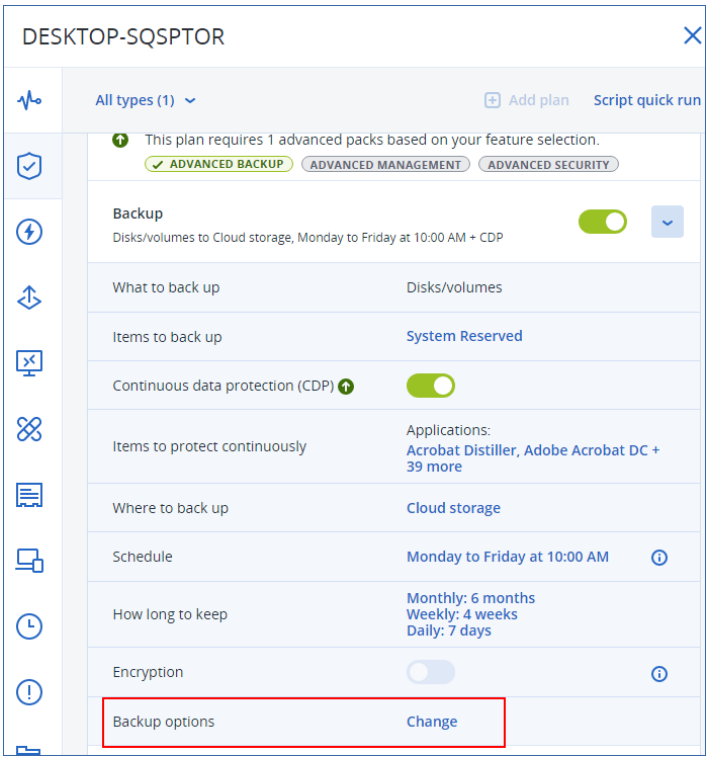
Odzyskiwanie jednym kliknięciem to opcja tworzenia kopii zapasowych dostępna w planie ochrony. Dodatkowe informacje na temat tworzenia planu można znaleźć w sekcji "Tworzenie planu ochrony" (s. 222).

Uwaga
Włączenie funkcji Odzyskiwanie jednym kliknięciem powoduje włączenie również narzędzia Startup Recovery Manager na komputerze docelowym. Jeżeli włączenie narzędzia Startup Recovery Manager będzie niemożliwe, to operacja tworzenia kopii zapasowej na potrzeby funkcji Odzyskiwanie jednym kliknięciem zakończy się niepowodzeniem. Dodatkowe informacje na temat narzędzia Startup Recovery Manager można znaleźć w sekcji "Startup Recovery Manager" (s. 782).

Aby włączyć funkcję Odzyskiwanie jednym kliknięciem

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. W sekcji **Elementy uwzględniane w kopii zapasowej** wybierz **Cały komputer** lub **Dyski/woluminy**.
3. [W przypadku wybrania opcji **Dyski/woluminy**] W sekcji **Elementy uwzględniane w kopii zapasowej** wskaż dyski lub woluminy, które mają zostać uwzględnione w kopii zapasowej.
4. W sekcji **Opcje tworzenia kopii zapasowych** kliknij **Zmień**, a następnie wybierz **Odzyskiwanie jednym kliknięciem**.

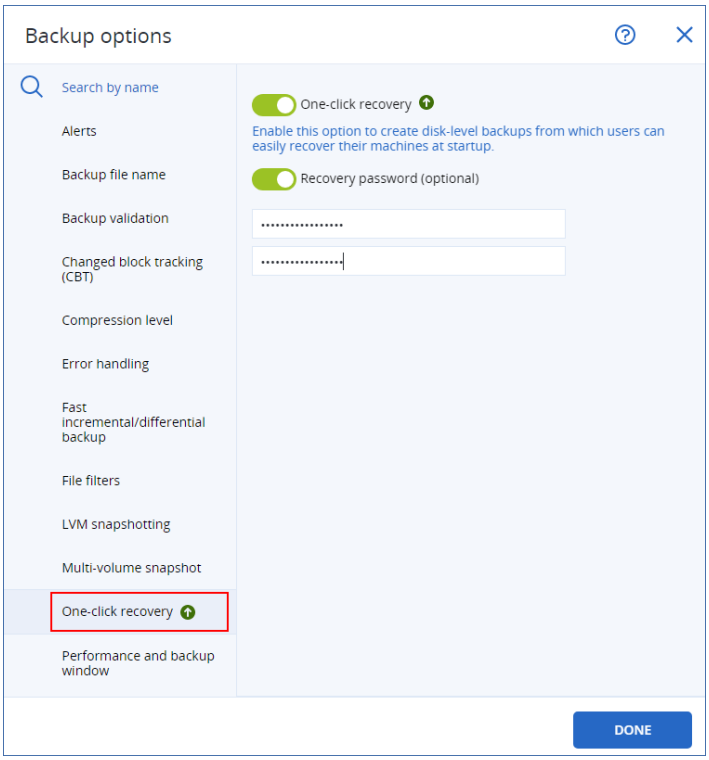
© Acronis International GmbH, 2003-2024



5. Włącz przełącznik **Odzyskiwanie jednym kliknięciem**.
6. [Opcjonalnie] Włącz przełącznik **Hasło odzyskiwania**, a następnie ustaw hasło.

Ważne
Zdecydowanie zalecamy ustawienie hasła odzyskiwania. Dopilnuj, aby użytkownik wykonujący operację odzyskiwania jednym kliknięciem na komputerze docelowym znał to hasło.

© Acronis International GmbH, 2003-2024



7. Kliknij **Gotowe**.
8. Skonfiguruj pozostałe elementy planu ochrony stosownie do potrzeb, a następnie zapisz plan.

W wyniku tych działań po uruchomieniu planu ochrony i utworzeniu kopii zapasowej funkcja Odzyskiwanie jednym kliknięciem będzie dostępna dla użytkowników chronionego komputera.

Ważne
Po zaktualizowaniu agenta ochrony odzyskiwanie jednym kliknięciem staje się tymczasowo niedostępne. Aby ponownie włączyć odzyskiwanie jednym kliknięciem, uruchom operację tworzenia kopii zapasowej. Po zakończeniu tworzenia kopii zapasowej znów będzie można przeprowadzać odzyskiwanie jednym kliknięciem.

Wyłączanie funkcji Odzyskiwanie jednym kliknięciem

Funkcję Odzyskiwanie jednym kliknięciem dla określonej maszyny można wyłączyć następująco:

- Wyłącz opcję **Odzyskiwanie jednym kliknięciem** w planie ochrony zastosowanym do tej maszyny.
- Odwołaj plan ochrony, w którym jest włączona opcja **Odzyskiwanie jednym kliknięciem**.
- Usuń plan ochrony, w którym jest włączona opcja **Odzyskiwanie jednym kliknięciem**.

© Acronis International GmbH, 2003-2024

Odzyskiwanie komputera przy użyciu funkcji Odzyskiwanie jednym kliknięciem

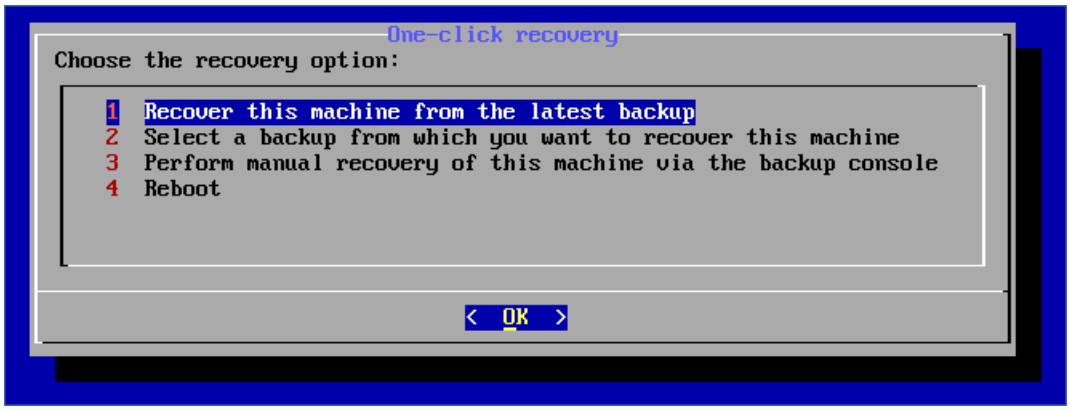
Wymagania wstępne

- Do komputera zastosowano plan ochrony z włączoną opcją tworzenia kopii zapasowych **Odzyskiwanie jednym kliknięciem**.
- Istnieje co najmniej jedna kopia zapasowa dysku komputera.

Aby odzyskać komputer

1. Uruchom ponownie komputer, który chcesz odzyskać.
2. Podczas uruchamiania ponownie naciśnij klawisz F11, aby otworzyć narzędzie Startup Recovery Manager.

   Zostanie otwarte okno nośnika ratunkowego.
3. Wybierz **Acronis Cyber Protect**.
4. [Jeśli w planie ochrony zostało ustawione hasło odzyskiwania] Wprowadź hasło odzyskiwania, a następnie kliknij **OK**.
5. Wybierz opcję funkcji Odzyskiwanie jednym kliknięciem.
   - Aby automatycznie odzyskać ostatnią kopię zapasową, wybierz pierwszą opcję, a następnie kliknij **OK**.
   - Aby odzyskać kolejną kopię zapasową dostępną w archiwum kopii zapasowych, wybierz drugą opcję, a następnie kliknij **OK**.

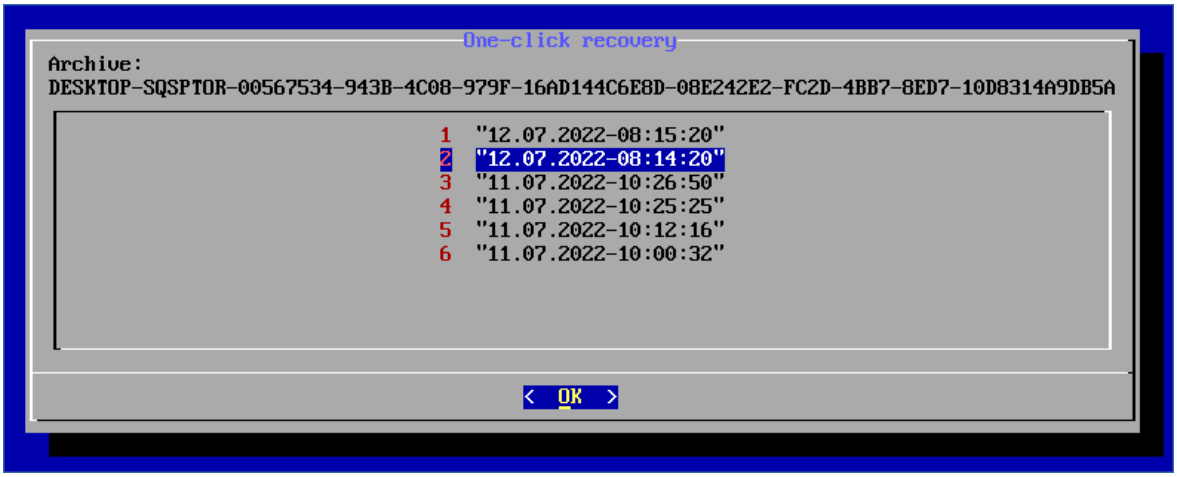


6. Potwierdź wybór, klikając **Tak**.

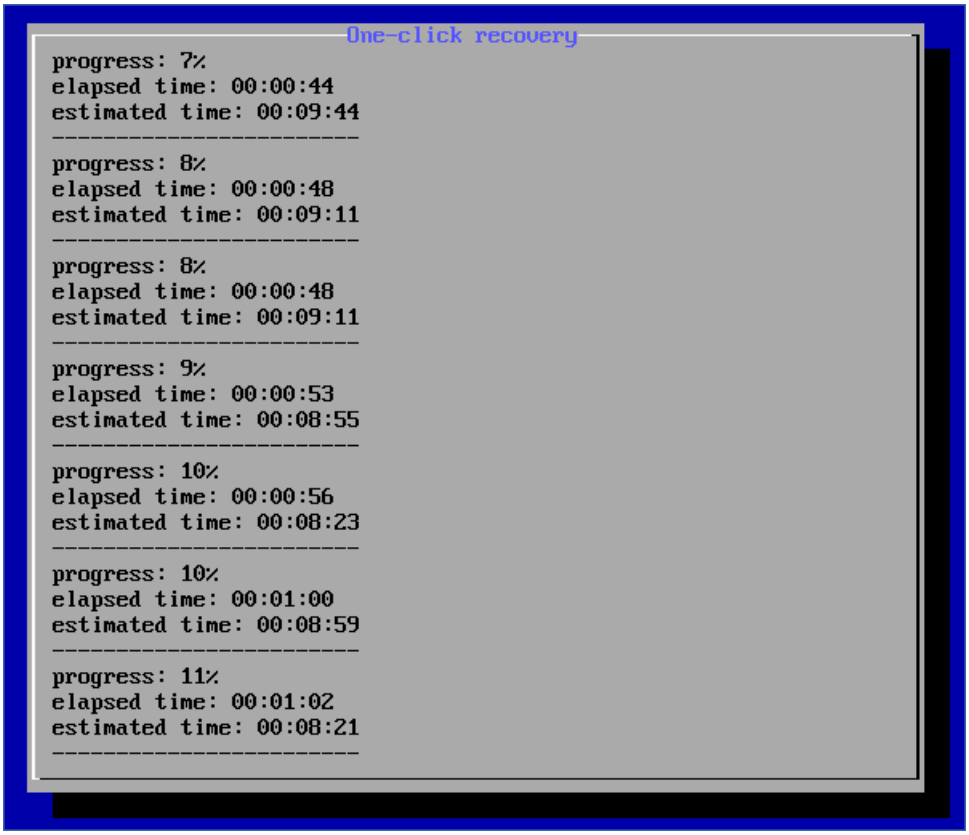
   Zostanie otwarte, a następnie zamknięte okno nośnika ratunkowego. Procedura odzyskiwania będzie kontynuowana bez nośnika.
7. [Jeśli chcesz odzyskać określoną kopię zapasową] Wybierz kopię zapasową, którą chcesz

© Acronis International GmbH, 2003-2024

odzyskać, a następnie kliknij **OK**.



Odzyskiwanie rozpocznie się po chwili i będzie pokazywany jego postęp. Po zakończeniu operacji odzyskiwania komputer zostanie uruchomiony ponownie.



Wydajność i okno na utworzenie kopii zapasowej

Ta opcja umożliwia ustawienie jednego z trzech poziomów wydajności tworzenia kopii zapasowej (wysoki, niski, zabroniony) dla każdej godziny w tygodniu. W ten sposób można definiować przedziały czasu, w których operacje tworzenia kopii zapasowych mogą być uruchamiane i wykonywane. Niski i wysoki poziom wydajności można też skonfigurować przez określenie priorytetu procesów i szybkości danych wyjściowych.

© Acronis International GmbH, 2003-2024

Opcja ta nie jest dostępna w przypadku operacji tworzenia kopii zapasowych wykonywanych przez agentów w chmurze, np. kopii zapasowych witryn internetowych lub kopii zapasowych serwerów znajdujących się w lokalizacji odzyskiwania w chmurze.

Ta opcja działa tylko w przypadku procesów tworzenia i replikacji kopii zapasowych. Polecenia następujące po utworzeniu kopii zapasowej i inne operacje uwzględnione w planie ochrony (na przykład sprawdzanie poprawności) będą wykonywane niezależnie od tej opcji.

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest wyłączona, operacje tworzenia kopii zapasowych mogą być uruchamiane w każdej chwili, z zastosowaniem następujących parametrów (bez względu na to, czy ich wartości zostały zmienione w stosunku do wartości predefiniowanych):

- Priorytet procesora: **Niski** (w systemie Windows odpowiada ustawieniu **Poniżej normalnego**)
- Szybkość danych wyjściowych: **Bez ograniczeń**

W przypadku włączenia tej opcji zaplanowane kopie zapasowe są dozwolone lub blokowane zgodnie z parametrami wydajności określonymi dla bieżącej godziny. Na początku godziny, w której kopie zapasowe są blokowane, proces tworzenia kopii zapasowych jest automatycznie zatrzymywany i jest generowany alert. Nawet jeśli zaplanowane kopie zapasowe zostaną zablokowane, tworzenie kopii zapasowej można rozpocząć ręcznie. Zostaną użyte parametry wydajności z ostatniej godziny, w której tworzenie kopii zapasowych było dozwolone.

Uwaga
Możesz skonfigurować wydajność i okno na utworzenie kopii zapasowej indywidualnie w przypadku każdej lokalizacji replikacji z osobna. Aby uzyskać dostęp do ustawień lokalizacji replikacji, kliknij w planie ochrony ikonę koła zębatego obok nazwy lokalizacji, a następnie kliknij **Wydajność i okno na utworzenie kopii zapasowej**.

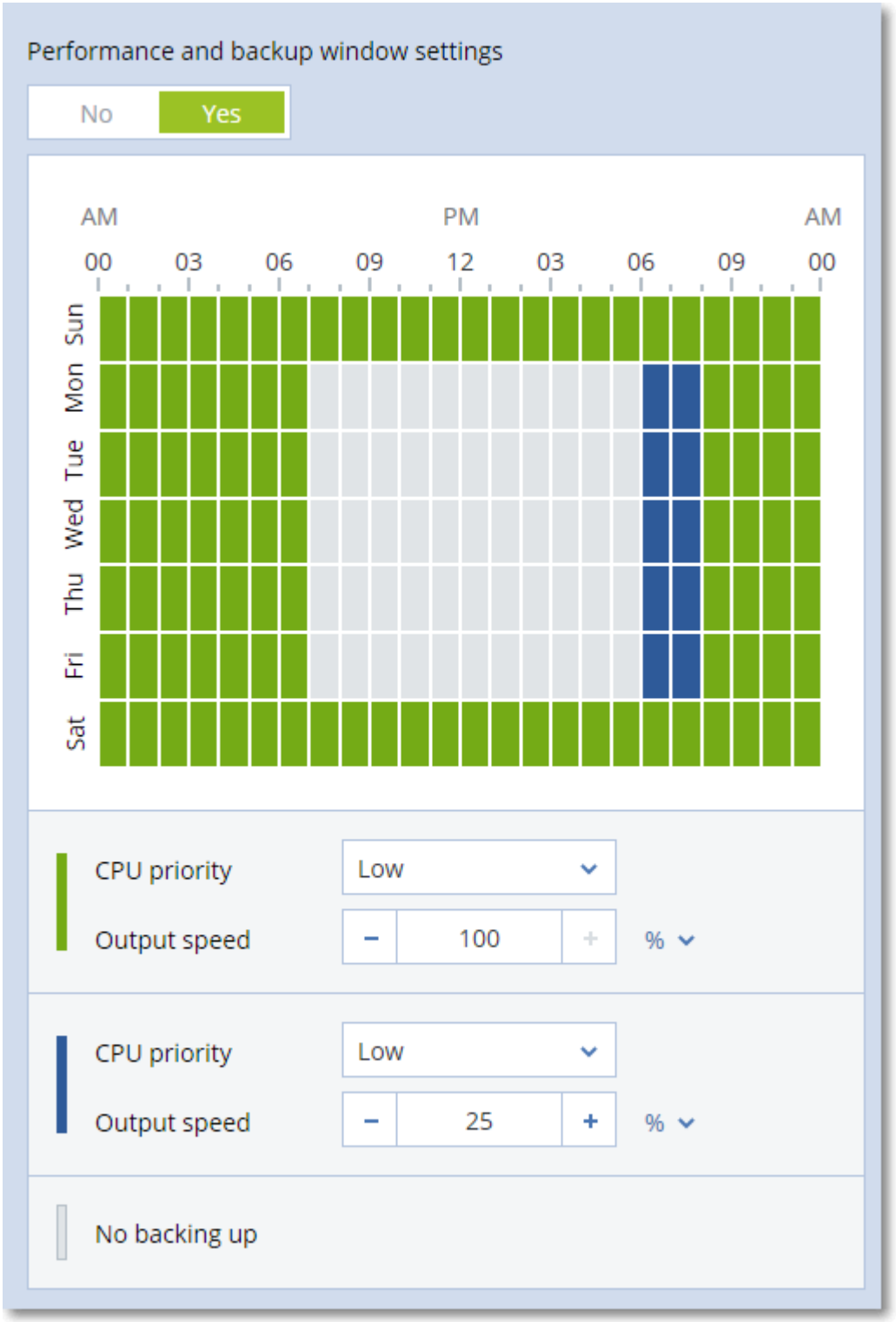
Okno na utworzenie kopii zapasowej

Każdy prostokąt odzwierciedla godzinę w dniu tygodnia. Klikaj prostokąt, aby przełączać między następującymi stanami:

- **Zielony:** operacja tworzenia kopii zapasowej jest dozwolona — z parametrami określonymi w zielonej sekcji poniżej.
- **Niebieski:** operacja tworzenia kopii zapasowej jest dozwolona — z parametrami określonymi w niebieskiej sekcji poniżej.
  Jeśli kopia zapasowa ma ustawiony format **Wersja 11**, ten stan jest niedostępny.
- **Szary:** operacja tworzenia kopii zapasowej jest blokowana.

Aby zmienić stan wielu prostokątów naraz, można kliknąć i przeciągnąć myszą.

© Acronis International GmbH, 2003-2024



Priorytet procesora

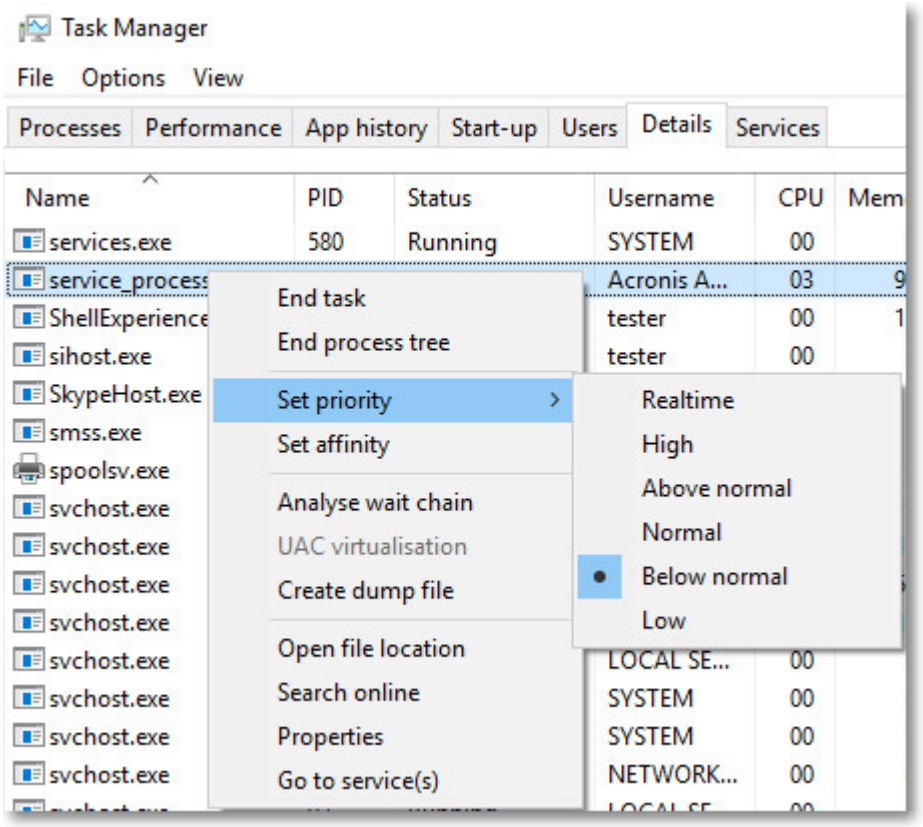
Ten parametr umożliwia określenie priorytetu procesu tworzenia kopii zapasowej w systemie operacyjnym.

Dostępne są następujące ustawienia: **Niski**, **Normalny**, **Wysoki**.

© Acronis International GmbH, 2003-2024

Priorytet procesu działającego w systemie określa ilość mocy obliczeniowej procesora i zasobów systemowych przydzielonych do tego procesu. Obniżenie priorytetu tworzenia kopii zapasowej zwolni więcej zasobów dla pozostałych aplikacji. Podwyższenie priorytetu tworzenia kopii zapasowej może przyspieszyć proces tworzenia kopii zapasowej przez żądanie przydzielenia przez system operacyjny większej ilości zasobów, takich jak moc obliczeniowa procesora, aplikacji tworzącej kopię zapasową. Jednak efekt takiej operacji będzie zależał od całkowitego wykorzystania mocy obliczeniowej procesora oraz innych czynników, takich jak szybkość odczytu/zapisu na dysku czy natężenie ruchu w sieci.

Ta opcja umożliwia ustawienie priorytetu procesu tworzenia kopii zapasowej (**service_process.exe**) w systemie Windows oraz parametru niceness procesu tworzenia kopii zapasowej (**service_process**) w systemach Linux i macOS.



Poniższa tabela zawiera zestawienie mapowania tego ustawienia w systemach Windows, Linux i macOS.

Priorytet w rozwiązaniu Cyber Protection	Priorytet w systemie Windows	Parametr niceness w systemach Linux i macOS
Niski	Poniżej normalnego	10
Normalny	Normalny	0
Wysoki	Wysoki	-10

© Acronis International GmbH, 2003-2024

Szybkość danych wyjściowych podczas tworzenia kopii zapasowej

Ten parametr umożliwia ograniczenie szybkości zapisu na dysku twardym (gdy kopia zapasowa jest tworzona w folderze lokalnym) lub szybkości przesyłania danych kopii zapasowej przez sieć (gdy kopia zapasowa jest tworzona w udziale sieciowym lub chmurze).

W przypadku włączenia tej opcji można określić maksymalną dozwoloną szybkość danych wyjściowych:

- Jako procent szacowanej szybkości zapisu na docelowym dysku twardym (gdy kopia zapasowa jest tworzona w folderze lokalnym) lub szacowanej maksymalnej szybkości połączenia sieciowego (gdy kopia zapasowa jest tworzona w udziale sieciowym lub chmurze).

  To ustawienie działa tylko wtedy, gdy agent jest uruchomiony w systemie Windows.
- W KB/s (w przypadku wszystkich lokalizacji docelowych).

Fizyczne dostarczanie danych

Ta opcja jest dostępna, jeśli miejscem docelowym kopii zapasowej lub replikacji jest chmura, a format kopii zapasowej jest ustawiony jako **Wersja 12**.

Ta opcja działa w przypadku kopii zapasowych na poziomie dysku i kopii zapasowych plików tworzonych przez agenta dla systemu Windows, agenta dla systemu Linux, agenta dla systemu Mac, agenta dla VMware, agenta dla Hyper-V oraz agenta dla Virtuozzo.

Ta opcja umożliwia przesłanie pierwszej pełnej kopii zapasowej utworzonej w ramach planu ochrony do chmury na dysku twardym przy użyciu usługi Fizyczne dostarczanie danych. Kolejne przyrostowe kopie zapasowe będą już wykonywane przez sieć.

W przypadku lokalnych kopii zapasowych, które są replikowane do chmury, przyrostowe kopie zapasowe są kontynuowane i zapisywane lokalnie do czasu przesłania początkowej kopii zapasowej do chmury. Potem wszystkie przyrostowe zmiany są replikowane do chmury zgodnie z harmonogramem tworzenia kopii zapasowych.

Ustawienie wstępne: **Wyłączono.**

Informacje o usłudze Fizyczne dostarczanie danych

Interfejs internetowy usługi Fizyczne dostarczanie danych jest dostępny tylko dla administratorów.

Szczegółowe instrukcje korzystania z usługi Fizyczne dostarczanie danych oraz narzędzie do tworzenia zleceń wysyłki można znaleźć w Podręczniku administratora usługi Fizyczne dostarczanie danych. W celu uzyskania dostępu do tego dokumentu w ramach interfejsu internetowego usługi Fizyczne dostarczanie danych kliknij ikonę ze znakiem zapytania.

© Acronis International GmbH, 2003-2024

Omówienie procesu fizycznego dostarczania danych

1. [Aby dostarczyć kopie zapasowe, których podstawową lokalizacją jest chmura]
   a. Utwórz nowy plan ochrony obejmujący tworzenie kopii zapasowych w chmurze.
   b. W wierszu **Opcje tworzenia kopii zapasowych** kliknij **Zmień**.
   c. Na liście dostępnych opcji kliknij **Fizyczne dostarczanie danych**.

   Kopie zapasowe można utworzyć bezpośrednio na wybranym dysku wymiennym albo w folderze lokalnym bądź sieciowym, a następnie skopiować lub przenieść na ten dysk.
2. [Aby dostarczyć lokalne kopie zapasowe, które są replikowane do chmury]

   Uwaga
   Ta opcja jest obsługiwana w przypadku agenta ochrony w wersji C21.06 lub nowszej.

   a. Utwórz nowy plan ochrony obejmujący tworzenie kopii zapasowych w magazynie lokalnym lub sieciowym.
   b. Kliknij **Dodaj lokalizację** i wybierz **Chmura**.
   c. W wierszu lokalizacji **Chmura** kliknij ikonę koła zębatego i wybierz **Fizyczne dostarczanie danych**.
3. W obszarze **Użyj usługi Fizyczne dostarczanie danych** kliknij **Tak** i **Gotowe**.
   Opcja Szyfrowanie zostanie automatycznie włączona w planie ochrony, ponieważ wszystkie dostarczane kopie zapasowe muszą być zaszyfrowane.
4. W wierszu **Szyfrowanie** kliknij **Określ hasło** i wprowadź hasło na potrzeby szyfrowania.
5. W wierszu **Fizyczne dostarczanie danych** wybierz dysk wymienny, na którym zapisano początkową kopię zapasową.
6. Kliknij **Utwórz**, aby zapisać plan ochrony.
7. Po utworzeniu pierwszej kopii zapasowej należy za pomocą interfejsu internetowego usługi Fizyczne dostarczanie danych pobrać narzędzie do tworzenia zamówień i utworzyć zamówienie.
   Aby uzyskać dostęp do tego interfejsu internetowego, zaloguj się w portalu zarządzania, kliknij **Przegląd** > **Wykorzystanie**, a następnie kliknij **Zarządzaj usługą** w obszarze **Fizyczne dostarczanie danych**.

   Ważne
   Po utworzeniu pierwszej pełnej kopii zapasowej kolejne kopie zapasowe muszą być tworzone w ramach tego samego planu ochrony. Inny plan ochrony, nawet mający takie same parametry i dotyczący tego samego komputera, będzie wymagać innego cyklu fizycznego dostarczania danych.
8. Zapakuj dyski i wyślij je do centrum danych.

© Acronis International GmbH, 2003-2024

Ważne
Koniecznie przestrzegaj instrukcji dotyczących pakowania zawartych w Podręczniku administratora usługi Fizyczne dostarczanie danych.

9. Status zamówienia możesz monitorować w interfejsie internetowym usługi Fizyczne dostarczanie danych. Pamiętaj, że dopóki pierwsza kopia zapasowa nie zostanie przesłana do chmury, kolejne operacje tworzenia kopii zapasowych będą się kończyć niepowodzeniem.

Polecenia poprzedzające/następujące

Ta opcja umożliwia określenie poleceń wykonywanych automatycznie przed utworzeniem kopii zapasowej i po jego zakończeniu.

Poniższy schemat przedstawia czas wykonania poleceń poprzedzających/następujących.

Polecenie poprzedzające utworzenie kopii zapasowej	Kopia zapasowa	Polecenie następujące po utworzeniu kopii zapasowej

Przykłady zastosowania poleceń poprzedzających/następujących:

- Usuwanie tymczasowych plików z dysku przed rozpoczęciem tworzenia kopii zapasowej.
- Konfigurowanie uruchamiania programu antywirusowego innego producenta przed każdym rozpoczęciem tworzenia kopii zapasowej.
- Wybiórcze kopiowanie kopii zapasowych do innej lokalizacji. Przydatność tej opcji polega na tym, że w ramach replikacji skonfigurowanej w planie ochrony *każda* kopia zapasowa jest kopiowana do kolejnych lokalizacji.

Agent przeprowadza replikację *po* wykonaniu polecenia następującego po utworzeniu kopii zapasowej.

Program nie obsługuje poleceń interaktywnych wymagających wpisania tekstu przez użytkownika (na przykład „pause”).

Polecenie poprzedzające utworzenie kopii zapasowej

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu tworzenia kopii zapasowej

1. Włącz przełącznik **Wykonaj polecenie przed utworzeniem kopii zapasowej**.
2. W polu **Polecenie** wpisz polecenie lub wybierz plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause”).
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby podaj argumenty wykonania polecenia.
5. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej

© Acronis International GmbH, 2003-2024

tabeli.

6. Kliknij **Gotowe**.

Pole wyboru	**Wybór**			
Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie twórz kopii zapasowej przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Utwórz kopię zapasową dopiero po pomyślnym wykonaniu polecenia. Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem.	Utwórz kopię zapasową po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N.d.	Utwórz kopię zapasową równolegle z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

* Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera.

Uwaga
Jeśli wykonanie skryptu się nie powiedzie z powodu konfliktu związanego z wymaganą wersją biblioteki w systemie Linux, wyklucz zmienne środowiskowe `LD_LIBRARY_PATH` i `LD_PRELOAD` przez dodanie do skryptu następujących wierszy:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Polecenie następujące po utworzeniu kopii zapasowej

Aby określić polecenie/plik wykonywalny, które mają zostać wykonane po zakończeniu tworzenia kopii zapasowej

© Acronis International GmbH, 2003-2024

1. Włącz przełącznik **Wykonaj polecenie po utworzeniu kopii zapasowej**.
2. W polu **Polecenie** wpisz polecenie lub wybierz plik wsadowy.
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
5. Jeśli pomyślne wykonanie polecenia ma znaczenie krytyczne, zaznacz pole wyboru **Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem**. Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera. W takim przypadku kopia zapasowa będzie miała status **Błąd**.

   Jeśli to pole wyboru nie jest zaznaczone, wynik wykonania polecenia nie wpływa na powodzenie lub niepowodzenie operacji tworzenia kopii zapasowej. Wynik wykonania polecenia można sprawdzić na karcie **Działania**.
6. Kliknij **Gotowe**.

Polecenia poprzedzające rejestrowanie danych/następujące po nim

Ta opcja umożliwia określenie poleceń, które mają zostać wykonane automatycznie przed zarejestrowaniem danych i po jego zakończeniu (czyli wykonaniu migawki danych). Dane są rejestrowane na początku procedury tworzenia kopii zapasowej.

Poniższy schemat przedstawia czas wykonania poleceń poprzedzających rejestrowanie danych i następujących po nim.

	<---------- **Kopia zapasowa** ---------->				
Polecenie poprzedzające utworzenie kopii zapasowej	Polecenie poprzedzające rejestrowanie danych	Rejestrowanie danych	Polecenie następujące po zarejestrowaniu danych	Zapisywanie danych w zestawie kopii zapasowych	Polecenie następujące po utworzeniu kopii zapasowej

Interakcja z innymi opcjami tworzenia kopii zapasowych

Wykonywanie poleceń poprzedzających rejestrowanie danych i następujących po nim może być modyfikowane przez inne opcje tworzenia kopii zapasowych.

Jeśli jest włączona opcja **Migawka wielowoluminowa**, polecenia poprzedzające rejestrowanie danych i następujące po nim zostaną wykonane tylko raz, ponieważ zostaną utworzone migawki wszystkich woluminów naraz. Jeśli opcja **Migawka wielowoluminowa** jest wyłączona, polecenia poprzedzające rejestrowanie danych i następujące po nim zostaną wykonane osobno dla każdego woluminu uwzględnianego w kopii zapasowej, ponieważ migawki będą tworzone po kolei, wolumin po woluminie.

© Acronis International GmbH, 2003-2024

Jeśli jest włączona opcja **Usługa kopiowania woluminów w tle (VSS)**, polecenia poprzedzające rejestrowanie danych i następujące po nim oraz czynności wykonywane przez Usługę kopiowania woluminów w tle będą wykonywane następująco:

Polecenia poprzedzające rejestrowanie danych > *Wstrzymanie VSS* > *Rejestrowanie danych* > *Wznowienie VSS* > *Polecenia następujące po rejestrowaniu danych*

Przy użyciu poleceń wykonywanych przed rejestrowaniem danych/następujących po nim można zawiesić lub wznowić działanie bazy danych lub aplikacji, która nie jest kompatybilna z usługą VSS. Ponieważ rejestracja danych trwa raptem kilka sekund, czas bezczynności baz danych lub aplikacji będzie naprawdę minimalny.

Polecenie poprzedzające rejestrowanie danych

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu rejestrowania danych

1. Włącz przełącznik **Wykonaj polecenie przed zarejestrowaniem danych**.
2. W polu **Polecenie** wpisz polecenie lub wybierz plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause”).
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby podaj argumenty wykonania polecenia.
5. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
6. Kliknij **Gotowe**.

Pole wyboru	**Wybór**			
Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie rejestruj danych przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Zarejestruj dane dopiero po	Zarejestruj dane po wykonaniu polecenia,	N.d.	Zarejestruj dane równolegle z wykonywaniem

© Acronis International GmbH, 2003-2024

	pomyślnym wykonaniu polecenia. Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem.	niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.		polecenia i niezależnie od wyniku jego wykonania.

* Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera.

Uwaga
Jeśli wykonanie skryptu się nie powiedzie z powodu konfliktu związanego z wymaganą wersją biblioteki w systemie Linux, wyklucz zmienne środowiskowe `LD_LIBRARY_PATH` i `LD_PRELOAD` przez dodanie do skryptu następujących wierszy:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

Polecenie następujące po zarejestrowaniu danych

Aby określić polecenie/plik wsadowy do wykonania po zarejestrowaniu danych

1. Włącz przełącznik **Wykonaj polecenie po zarejestrowaniu danych**.
2. W polu **Polecenie** wpisz polecenie lub wybierz plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause”).
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby podaj argumenty wykonania polecenia.
5. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
6. Kliknij **Gotowe**.

Pole wyboru	Wybór			
Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie twórz kopii zapasowej przed zakończeniem	Wybrane	Wybrane	Niewybrane	Niewybrane

© Acronis International GmbH, 2003-2024

wykonywania polecenia				
Wynik				
	Ustawienie wstępne Kontynuuj tworzenie kopii zapasowej dopiero po pomyślnym wykonaniu polecenia.	Kontynuuj tworzenie kopii zapasowej po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N.d.	Kontynuuj tworzenie kopii zapasowej równolegle z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

* Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera.

Tworzenie harmonogramu

Ta opcja umożliwia określenie, czy tworzenie kopii zapasowych ma się rozpoczynać ściśle zgodnie z harmonogramem, czy z opóźnieniem, a także określenie liczby maszyn wirtualnych uwzględnianych jednocześnie w kopii zapasowej.

Dokładniejsze instrukcje dotyczące konfigurowania harmonogramu tworzenia kopii zapasowych można znaleźć w sekcji "Uruchamianie operacji tworzenia kopii zapasowej zgodnie z harmonogramem" (s. 450).

Ustawienie wstępne: **Rozłóż uruchamianie operacji tworzenia kopii zapasowych w przedziale czasu**. **Maksymalne opóźnienie**: **30 minut**.

Można wybrać jedną z następujących opcji:

- **Rozpocznij wszystkie operacje tworzenia kopii zapasowych dokładnie według harmonogramu**
  Tworzenie kopii zapasowych komputerów fizycznych będzie się rozpoczynać zgodnie z harmonogramem. Kopie zapasowe maszyn wirtualnych będą tworzone pojedynczo.
- **Rozłóż uruchamianie w przedziale czasu**
  Tworzenie kopii zapasowych komputerów fizycznych będzie się rozpoczynać z opóźnieniem w stosunku do zaplanowanego czasu. Wartość opóźnienia jest w przypadku każdego komputera wybierana losowo i mieści się w zakresie od zera do określonej przez Ciebie wartości maksymalnej. Ustawienia tego warto użyć w przypadku tworzenia kopii zapasowych wielu komputerów w lokalizacji sieciowej — pozwoli ono uniknąć nadmiernego obciążenia sieci. Wartość opóźnienia dla poszczególnych komputerów jest ustalana podczas stosowania planu ochrony na tych komputerach. Pozostaje ona niezmienna do chwili ewentualnej edycji planu ochrony i zmiany maksymalnej wartości opóźnienia.
  Kopie zapasowe maszyn wirtualnych będą tworzone pojedynczo.
- **Ogranicz liczbę jednoczesnych operacji tworzenia kopii zapasowych o**

© Acronis International GmbH, 2003-2024

Użyj tej opcji, aby zarządzać równoległymi operacjami tworzenia kopii zapasowych maszyn wirtualnych, których kopie zapasowe są tworzone na poziomie hiperwizora (bezagentowe tworzenie kopii zapasowych).

Plany ochrony, w których wybrano tę opcję, mogą być wykonywane razem z innymi planami ochrony obsługiwanymi przez tego samego agenta w tym samym czasie. Po wybraniu tej opcji należy określić liczbę równoległych operacji tworzenia kopii zapasowych na plan. Łączna liczba maszyn, których kopie zapasowe są tworzone w tym samym czasie przez wszystkie plany, jest ograniczona do 10 na agenta. Informacje na temat zmieniania limitu domyślnego można znaleźć w sekcji "Ograniczanie łącznej liczby maszyn wirtualnych, których kopie zapasowe mogą być tworzone w tym samym czasie" (s. 753).

Plany ochrony, w których ta opcja nie jest wybrana, uruchamiają operacje tworzenia kopii zapasowych sekwencyjnie, jedna maszyna wirtualna po drugiej.

Kopia zapasowa sektor po sektorze

Ta opcja jest dostępna tylko w przypadku kopii zapasowych na poziomie dysku.

Opcja umożliwia określenie, czy ma zostać utworzona dokładna kopia dysku lub woluminu na poziomie fizycznym.

Ustawienie wstępne: **Wyłączono**.

W przypadku włączenia tej opcji w kopii zapasowej zostaną uwzględnione wszystkie sektory dysku lub woluminu, w tym nieprzydzielone miejsce oraz sektory bez danych. Wynikowa kopia zapasowa będzie miała taki sam rozmiar jak uwzględniony w niej dysk (jeśli opcja „Stopień kompresji” ma wartość **Brak**). W przypadku tworzenia kopii zapasowej dysków z nierozpoznanym lub nieobsługiwanym systemem plików oprogramowanie automatycznie przełącza się na tryb „sektor po sektorze”.

Uwaga
Nie będzie można odzyskać danych aplikacji z kopii zapasowych utworzonych w trybie sektor po sektorze.

Dzielenie

Opcja umożliwia wybranie metody dzielenia dużych kopii zapasowych na mniejsze pliki.

Uwaga
Funkcja dzielenia nie jest dostępna w planach ochrony, w których lokalizacją kopii zapasowych jest chmura.

Ustawienie wstępne:

- Jeśli lokalizacją kopii zapasowych jest folder lokalny lub sieciowy (SMB), a formatem kopii zapasowej jest Wersja 12: **Stały rozmiar — 200 GB**

© Acronis International GmbH, 2003-2024

To ustawienie umożliwia oprogramowaniu do tworzenia kopii zapasowych pracę z dużymi ilościami danych w systemie plików NTFS bez negatywnych skutków fragmentacji plików.

- W przeciwnym razie: **Automatycznie**

Dostępne są poniższe ustawienia:

- **Automatycznie**
  Jeśli rozmiar kopii zapasowej przekroczy maksymalny rozmiar pliku obsługiwany przez dany system plików, kopia zapasowa zostanie podzielona.
- **Stały rozmiar**
  Wprowadź wymagany rozmiar pliku lub wybierz go z listy rozwijanej.

Obsługa niepowodzenia zadania

Ta opcja określa zachowanie programu w sytuacji, gdy nie uda się wykonać planu ochrony zgodnie z harmonogramem lub komputer zostanie uruchomiony ponownie w czasie operacji tworzenia kopii zapasowej. Nie jest ona uwzględniana, jeśli plan ochrony zostanie uruchomiony ręcznie.

W przypadku włączenia tej opcji program jeszcze raz spróbuje wykonać plan ochrony. Można określić liczbę prób oraz odstępy między nimi. Program przestanie podejmować próby, gdy jedna z nich zakończy się pomyślnie lub po wykonaniu określonej liczby prób, w zależności od tego, który z tych warunków zostanie spełniony wcześniej.

Jeśli ta opcja jest włączona i komputer zostanie uruchomiony ponownie podczas operacji tworzenia kopii zapasowej, operacja ta nie zakończy się niepowodzeniem. Kilka minut po ponownym uruchomieniu operacja tworzenia kopii zapasowej zostanie automatycznie wznowiona — plik kopii zapasowej zostanie uzupełniony o brakujące dane. W tym scenariuszu zastosowania opcja **Odstęp między próbami** nie jest istotna.

Ustawienie wstępne: **Włączono**.

Uwaga
Ta opcja nie działa w przypadku kopii zapasowych na potrzeby analizy śledczej.

Warunki uruchomienia zadania

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux.

Opcja określa działanie programu w sytuacji, gdy ma się rozpocząć jakieś zadanie (zbliża się zaplanowany termin lub wystąpiło zdarzenie określone w harmonogramie), ale warunek (lub jeden z wielu warunków) nie został spełniony. Dodatkowe informacje o warunkach można znaleźć w sekcji "Warunki rozpoczęcia" (s. 457).

Ustawienie wstępne: **Poczekaj na spełnienie warunków z harmonogramu.**

© Acronis International GmbH, 2003-2024

Poczekaj na spełnienie warunków z harmonogramu

Przy tym ustawieniu funkcja harmonogramu rozpocznie monitorowanie warunków i uruchomi zadanie bezpośrednio po ich spełnieniu. Jeśli warunki nie zostaną w ogóle spełnione, zadanie nie zostanie uruchomione.

Jeśli warunki pozostają niespełnione przez zbyt długi czas i dalsze opóźnianie zadania staje się ryzykowne, można wyznaczyć czas, po upływie którego zadanie zostanie uruchomione niezależnie od warunku. Zaznacz pole wyboru **Uruchom zadanie mimo to po upływie** i podaj czas. Zadanie zostanie uruchomione niezwłocznie po spełnieniu warunków LUB po upływie maksymalnego czasu opóźnienia, w zależności od tego, która z tych sytuacji wystąpi wcześniej.

Pomiń wykonywanie zadania

Opóźnienie zadania może być niedopuszczalne, na przykład wtedy, gdy zadanie musi zostać wykonane dokładnie o określonej godzinie. Wówczas rozsądniej jest pominąć zadanie, zamiast czekać na spełnienie warunków, zwłaszcza w przypadku stosunkowo częstych zadań.

Usługa kopiowania woluminów w tle (VSS)

Ta opcja ma zastosowanie tylko w systemach operacyjnych Windows.

Określa ona, czy może być wykonana kopia zapasowa w sytuacji, gdy przynajmniej jeden procesów zapisywania w usłudze kopiowania woluminów w tle zakończy się błędem, oraz który dostawca ma powiadamiać aplikacje obsługujące technologię VSS rozpoczęciu tworzenia kopii zapasowej.

Usługa kopiowania woluminów w tle umożliwia zapewnienie spójnego stanu wszystkich danych używanych przez aplikacje, a zwłaszcza dokończenie wszystkich transakcji baz danych w momencie utworzenia migawki danych przez oprogramowanie do tworzenia kopii zapasowych. Spójność danych zapewnia z kolei możliwość odzyskania aplikacji w prawidłowym stanie i umożliwia rozpoczęcie jej używania natychmiast po odzyskaniu.

Migawka jest używana tylko podczas operacji tworzenia kopii zapasowej i jest automatycznie usuwana po zakończeniu tej operacji. Nie są przechowywane żadne pliki tymczasowe.

Aby zapewnić spójność danych uwzględnianych w kopii zapasowej, można użyć także Poleceń poprzedzających rejestrowanie danych oraz poleceń następujących po nim. Można na przykład określić polecenia poprzedzające rejestrowanie danych, które spowodują wstrzymanie działania bazy danych i wyczyszczenie pamięci podręcznej w celu dokończenia wszystkich transakcji, a następnie polecenia po rejestrowaniu danych, które spowodują wznowienie działania bazy danych po utworzeniu migawki.

© Acronis International GmbH, 2003-2024

Uwaga
Dla plików i folderów określonych w kluczu rejestru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** kopia zapasowa nie jest tworzona. W szczególności dla plików danych offline programu Outlook (.ost) nie tworzy się kopii zapasowej, ponieważ są one określone w wartości **OutlookOST** tego klucza.

Ignoruj składniki zapisywania usługi VSS zakończone niepowodzeniem

Można wybrać jedną z następujących opcji:

- **Ignoruj składniki zapisywania usługi VSS zakończone niepowodzeniem**
  Jeśli ta opcja będzie włączona, możliwe będzie pomyślne uzyskiwanie kopii zapasowych w przypadku, gdy składniki zapisywania usługi VSS zakończą się niepowodzeniem.

  Ważne
  Tworzenie kopii zapasowych uwzględniających aplikacje będzie zawsze kończyło się niepowodzeniem, jeśli wystąpi błąd w składniku zapisywania uwzględniającego aplikacje. Na przykład, jeśli tworzysz kopię zapasową uwzględniającą aplikacje dla danych SQL Server, a składnik **SqlServerWriter** zakończy się niepowodzeniem, to operacja tworzenia kopii zapasowej również zakończy się niepowodzeniem.

  Jeśli ta opcja będzie włączona, wykonywane są maksymalnie trzy kolejne próby wykonania migawki VSS.
  W pierwszej próbie wymagane są wszystkie składniki zapisywania usługi VSS. Jeśli ta próba zakończy się niepowodzeniem, zostanie powtórzona. Gdy druga próba również zakończy się niepowodzeniem, to składniki zapisywania usługi VSS z błędami zostaną wyłączone z operacji tworzenia kopii zapasowej i zostanie podjęta trzecia próba. W razie powodzenia trzeciej próby, proces tworzenia kopii zapasowej zostanie zakończony z ostrzeżeniem dotyczącym błędów w składnikach zapisywania usługi VSS. Jeśli trzecia próba nie będzie pomyślna, operacja tworzenia kopii zapasowej zostanie zakończona niepowodzeniem.
- **Wymagaj pomyślnego przetwarzania w przypadku wszystkich składników zapisywania usługi VSS**
  Jeśli jakikolwiek składnik zapisywania usługi VSS zakończy się niepowodzeniem, operacja tworzenia kopii zapasowej również zakończy się niepowodzeniem.

Wybierz dostawcę migawek

Można wybrać jedną z następujących opcji:

- **Automatycznie wybierz dostawcę migawek**
  Automatycznie wybierz między sprzętowym dostawcą migawek, programowymi dostawcami migawek a Dostawcą kopiowania w tle oprogramowania firmy Microsoft.
- **Użyj dostawcy kopiowania w tle oprogramowania firmy Microsoft**

© Acronis International GmbH, 2003-2024

Zaleca się wybranie tej opcji w przypadku tworzenia kopii zapasowych serwerów aplikacji (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint lub Active Directory).

Włącz tworzenie pełnych kopii zapasowych z usługą VSS

Jeśli ta opcja będzie włączona, dzienniki programu Microsoft Exchange Server i innych aplikacji uwzględniających usługę VSS (z wyjątkiem programu Microsoft SQL Server) będą obcinane po każdym pomyślnym utworzeniu pełnej, przyrostowej lub różnicowej kopii zapasowej na poziomie dysku.

Ustawienie wstępne: **Wyłączone**.

Opcja ta powinna być wyłączona w następujących przypadkach:

- Jeśli do tworzenia kopii zapasowych danych programu Exchange Server jest używany agent dla programu Exchange lub program innego producenta. W takim przypadku obcinanie dziennika będzie wpływało na kolejne kopie zapasowe dziennika transakcji.
- Jeśli do tworzenia kopii zapasowych danych SQL Server jest używany program innego producenta. Wynika to z faktu, że program innego producenta uzna wynikową kopię zapasową na poziomie dysku za „własną" pełną kopię. Dlatego utworzenie kolejnej różnicowej kopii zapasowej danych SQL Server zakończy się niepowodzeniem. Tworzenie kopii zapasowych będzie kończyło się niepowodzeniem do czasu, aż program innego producenta utworzy kolejną „własną" pełną kopię zapasową.
- Jeśli na komputerze są uruchomione inne aplikacje uwzględniające usługę VSS i z jakiegoś powodu chcesz zachować ich dzienniki.

Ważne
Włączenie tej opcji nie powoduje obcinania dzienników programu Microsoft SQL Server. Aby dziennik programu SQL Server był obcinany po utworzeniu kopii zapasowej, włącz opcję tworzenia kopii zapasowych Obcinanie dziennika.

Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych

Opcja umożliwia określenie, czy są wykonywane wyciszone migawki maszyny wirtualnej.

Ustawienie wstępne: **Włączono**.

W przypadku wyłączenia tej opcji wykonywana jest niewyciszona migawka. Maszyna wirtualna zostanie uwzględniona w kopii zapasowej w stanie spójności po awarii.

W przypadku włączenia tej opcji najpierw zostaną ukończone transakcje wszystkich aplikacji uwzględniających usługę VSS działających na maszynie wirtualnej, a potem zostanie wykonana wyciszona migawka.

Jeśli po liczbie prób określonej za pomocą opcji „Obsługa błędów" nie uda się wykonać wyciszonej migawki, a jest włączone tworzenie kopii zapasowych aplikacji, operacja tworzenia kopii zapasowej się nie powiedzie.

© Acronis International GmbH, 2003-2024

Jeśli po liczbie prób określonej za pomocą opcji „Obsługa błędów" nie uda się wykonać wyciszonej migawki, a jest wyłączone tworzenie kopii zapasowych aplikacji, zostanie utworzona kopia zapasowa spójna ze stanem awarii. Aby operacja tworzenia kopii zapasowej zakończyła się niepowodzeniem, a nie utworzeniem kopii zapasowej zgodnej ze stanem awarii, zaznacz pole wyboru **Jeśli wykonanie wyciszonej migawki nie jest możliwe, operacja tworzenia kopii zapasowej ma się zakończyć niepowodzeniem**.

W poniższej tabeli zestawiono dostępne ustawienia i ich efekty.

Ustawienia	Wyciszona migawka została pomyślnie wykonana		Wyciszona migawka nie została wykonana	
	Włączono tworzenie kopii zapasowych aplikacji	**Wyłączono tworzenie kopii zapasowych aplikacji**	**Włączono tworzenie kopii zapasowych aplikacji**	**Wyłączono tworzenie kopii zapasowych aplikacji**
Włączono opcję **Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych** Nie zaznaczono pola wyboru **Jeśli wykonanie wyciszonej migawki nie jest możliwe, operacja tworzenia kopii zapasowej ma się zakończyć niepowodzeniem**	Zostaje wykonana wyciszona migawka. Zostaje utworzona kopia zapasowa spójna z aplikacjami.	Zostaje wykonana wyciszona migawka. Zostaje utworzona kopia zapasowa spójna z aplikacjami.	Operacja tworzenia kopii zapasowej kończy się niepowodzeniem.	Zostaje wykonana niewyciszona migawka. Zostaje utworzona kopia zapasowa spójna ze stanem awarii.
Włączono opcję **Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych** Zaznaczono pole wyboru **Jeśli wykonanie wyciszonej migawki nie jest możliwe, operacja tworzenia kopii zapasowej ma się**	Zostaje wykonana wyciszona migawka. Zostaje utworzona kopia zapasowa spójna z aplikacjami.	Zostaje wykonana wyciszona migawka. Zostaje utworzona kopia zapasowa spójna z aplikacjami.	Operacja tworzenia kopii zapasowej kończy się niepowodzeniem.	Operacja tworzenia kopii zapasowej kończy się niepowodzeniem.

© Acronis International GmbH, 2003-2024

Ustawienia	Wyciszona migawka została pomyślnie wykonana		Wyciszona migawka nie została wykonana	
	Włączono tworzenie kopii zapasowych aplikacji	**Wyłączono tworzenie kopii zapasowych aplikacji**	**Włączono tworzenie kopii zapasowych aplikacji**	**Wyłączono tworzenie kopii zapasowych aplikacji**
zakończyć niepowodzeniem				
Wyłączono opcję **Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych**	Zostaje wykonana niewyciszona migawka. Zostaje utworzona kopia zapasowa spójna ze stanem awarii.	Zostaje wykonana niewyciszona migawka. Zostaje utworzona kopia zapasowa spójna ze stanem awarii.	Zostaje wykonana niewyciszona migawka. Zostaje utworzona kopia zapasowa spójna ze stanem awarii.	Zostaje wykonana niewyciszona migawka. Zostaje utworzona kopia zapasowa spójna ze stanem awarii.

Włączenie opcji **Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych** wyzwala też ewentualne skrypty poprzedzające zablokowanie i następujące po odblokowaniu znajdujące się na maszynie wirtualnej uwzględnianej w kopii zapasowej. Dodatkowe informacje o tych skryptach można znaleźć w sekcji "Automatyczne uruchamianie skryptów poprzedzających zablokowanie i następujących po odblokowaniu" (s. 742).

Aby wykonać wyciszoną migawkę, oprogramowanie do tworzenia kopii zapasowych używa modułu VSS w ramach maszyny wirtualnej, korzystając odpowiednio z narzędzi VMware Tools, usług integracji Hyper-V, narzędzi Virtuozzo Guest Tools, narzędzi Red Hat Virtualization Guest Tools lub narzędzi QEMU Guest Tools.

Uwaga
W przypadku maszyn wirtualnych Red Hat Virtualization (oVirt) warto zainstalować narzędzia QEMU Guest Tools, a nie Red Hat Virtualization Guest Tools. Niektóre wersje narzędzi Red Hat Virtualization Guest Tools nie obsługują migawek spójnych z aplikacjami.

Ta opcja nie ma wpływu na maszyny wirtualne Scale Computing HC3. W ich przypadku wyciszenie zależy od tego, czy na maszynie wirtualnej są zainstalowane narzędzia Scale Tools.

Tygodniowa kopia zapasowa

Ta opcja umożliwia wskazanie, które kopie zapasowe należy uznać za „tygodniowe” w regułach przechowywania i schematach tworzenia kopii zapasowych. „Tygodniową” kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu tygodnia.

Ustawienie wstępne: **Poniedziałek**.

Dziennik zdarzeń systemu Windows

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

© Acronis International GmbH, 2003-2024

Ta opcja umożliwia określenie, czy agenty muszą rejestrować zdarzenia operacji tworzenia kopii zapasowych w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, uruchom plik eventvwr.exe lub wybierz **Panel sterowania** > **Narzędzia administracyjne** > **Podgląd zdarzeń**). Zdarzenia, które mają być rejestrowane, można filtrować.

Ustawienie wstępne: **Wyłączono**.

Odzyskiwanie

Odzyskiwanie — ściągawka

W poniższej tabeli zestawiono dostępne metody odzyskiwania. Dzięki niej wybierzesz optymalną metodę odzyskiwania.

Uwaga
W przypadku dzierżawców w trybie zgodności nie można odzyskiwać kopii zapasowych w konsoli Cyber Protect. Więcej informacji na temat odzyskiwania takich kopii zapasowych można znaleźć w sekcji "Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności" (s. 1182).

Elementy do odzyskania	Metoda odzyskiwania
Komputer fizyczny (z systemem Windows lub Linux)	Przy użyciu konsoli Cyber Protect Przy użyciu nośnika startowego
Komputer fizyczny (z systemem Mac)	Przy użyciu nośnika startowego
Maszyna wirtualna (VMware, Hyper-V, Red Hat Virtualization [oVirt] lub Scale Computing HC3)	Przy użyciu konsoli Cyber Protect Przy użyciu nośnika startowego
Maszyna wirtualna lub kontener (Virtuozzo, Virtuozzo Hybrid Server lub Virtuozzo Hybrid Infrastructure)	Przy użyciu konsoli Cyber Protect
Konfiguracja ESXi	Przy użyciu nośnika startowego
Pliki/foldery	Przy użyciu konsoli Cyber Protect Pobieranie plików z chmury Przy użyciu nośnika startowego Wyodrębnianie plików z lokalnych kopii zapasowych
Stan systemu	Przy użyciu konsoli Cyber Protect

© Acronis International GmbH, 2003-2024

Bazy danych SQL	Przy użyciu konsoli Cyber Protect
Bazy danych programu Exchange	Przy użyciu konsoli Cyber Protect
Skrzynki pocztowe programu Exchange	Przy użyciu konsoli Cyber Protect
Witryny internetowe	Przy użyciu konsoli Cyber Protect
Microsoft 365	
Skrzynki pocztowe (lokalny agent dla usługi Microsoft 365)	Przy użyciu konsoli Cyber Protect
Skrzynki pocztowe (chmurowy agent dla usługi Microsoft 365)	Przy użyciu konsoli Cyber Protect
Foldery publiczne	Przy użyciu konsoli Cyber Protect
Pliki w usłudze OneDrive	Przy użyciu konsoli Cyber Protect
Dane programu SharePoint Online	Przy użyciu konsoli Cyber Protect
Google Workspace	
Skrzynki pocztowe	Przy użyciu konsoli Cyber Protect
Pliki z dysku Google	Przy użyciu konsoli Cyber Protect
Pliki z Dysku udostępnionego	Przy użyciu konsoli Cyber Protect

Odzyskiwanie na inną platformę

Odzyskiwanie na inną platformę jest dostępne w przypadku kopii zapasowych całych komputerów i kopii zapasowych dysków zawierających system operacyjny.

Odzyskiwanie na inną platformę jest przeprowadzane w następujących przypadkach:

- Kopia zapasowa została utworzona przez agenta jednego typu, ale jest odzyskiwana przez agenta drugiego typu.
- Kopia zapasowa utworzona przy użyciu agenta jest odzyskiwana na poziomie hiperwizora (odzyskiwanie bezagentowe) lub kopia zapasowa utworzona bezagentowo jest odzyskiwana przez agenta (odzyskiwanie przy użyciu agenta).
- Kopia zapasowa jest odzyskiwana na komputerze o innej konfiguracji sprzętowej (dotyczy to też sprzętu wirtualnego).

© Acronis International GmbH, 2003-2024

Uwaga
Niektóre urządzenia peryferyjne, na przykład drukarki, mogą nie zostać poprawnie odzyskane w przypadku odzyskiwania na inną platformę.

W poniższej tabeli przedstawiono kilka przykładów odzyskiwania na inną platformę.

Odzyskiwanie na inną platformę	
Kopia zapasowa utworzona bezagentowo	Odzyskiwanie przy użyciu agenta
Kopia zapasowa utworzona przy użyciu agenta	Odzyskiwanie bezagentowe
Kopia zapasowa utworzona przy użyciu agenta dla systemu Windows	Odzyskiwanie przy użyciu agenta dla VMware
Kopia zapasowa utworzona przy użyciu agenta dla VMware	Odzyskiwanie przy użyciu agenta dla Hyper-V
Kopia zapasowa utworzona przy użyciu agenta dla systemu Windows zainstalowanego na maszynie wirtualnej VMware ESXi	Odzyskiwanie przy użyciu agenta dla VMware (bezagentowe) na tym samym hoście VMware ESXi
Kopia zapasowa utworzona przy użyciu agenta dla systemu Windows	Kopia zapasowa utworzona przy użyciu agenta dla systemu Windows zainstalowanego na komputerze o innej konfiguracji sprzętowej
Kopia zapasowa komputera fizycznego	Odzyskiwanie jako maszynę wirtualną

Uwaga dla użytkowników komputerów Mac

- Począwszy od wersji 10.11 El Capitan, niektóre pliki systemowe, foldery i procesy są oflagowane do ochrony przy użyciu rozszerzonego atrybutu pliku com.apple.rootless. Funkcja ta jest nazywana ochroną integralności systemu (System Integrity Protection, SIP). Chronione pliki obejmują preinstalowane aplikacje oraz większość folderów w folderach /system, /bin, /sbin, /usr.
  Chronione pliki i foldery nie mogą zostać zastąpione podczas operacji odzyskiwania w ramach tego systemu operacyjnego. Jeśli zechcesz zastąpić chronione pliki, przeprowadź operację odzyskiwania przy użyciu nośnika startowego.
- Począwszy od systemu macOS Sierra 10.12, funkcja Store in Cloud może przenosić rzadko używane pliki do środowiska iCloud. W systemie plików pozostają niewielkie „odciski" tych plików i to one są uwzględniane w kopii zapasowej zamiast pierwotnych plików.
  Po odzyskaniu odcisku do oryginalnej lokalizacji jest on synchronizowany z usługą iCloud, dzięki czemu pierwotny plik staje się znów dostępny. Po odzyskaniu odcisku do innej lokalizacji nie można go zsynchronizować z usługą iCloud, wskutek czego pierwotny plik będzie niedostępny.

© Acronis International GmbH, 2003-2024

Bezpieczne odzyskiwanie

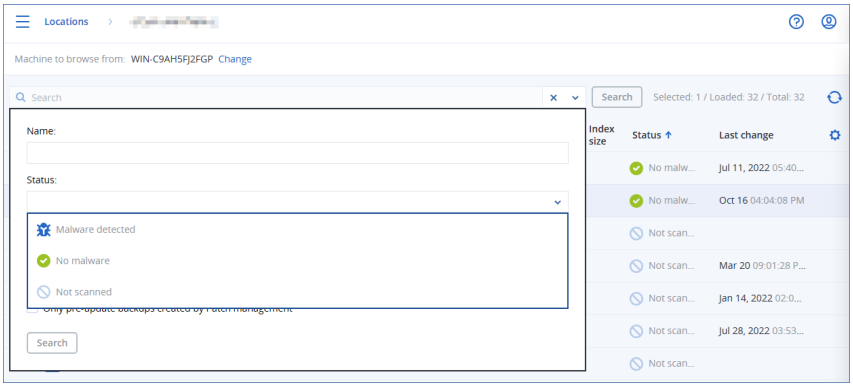
Skorzystaj z funkcji bezpiecznego odzyskiwania dostępnej w przypadku kopii zapasowych typu **Cały komputer** lub **Dyski/woluminy** obciążeń z systemem Windows, aby mieć pewność, że zostaną odzyskane tylko dane wolne od złośliwego oprogramowania, nawet jeśli kopia zapasowa zawiera zainfekowane pliki.

Podczas operacji bezpiecznego odzyskiwania kopia zapasowa jest automatycznie skanowana pod kątem złośliwego oprogramowania. Następnie agent ochrony odzyskuje kopię zapasową na obciążeniu docelowym, ale usuwa wszystkie zainfekowane pliki. W wyniku tego odzyskiwana jest kopia zapasowa bez złośliwego oprogramowania.

Ponadto kopii zapasowej zostanie przypisany jeden z następujących statusów:

- Wykryto złośliwe oprogramowanie
- Brak złośliwego oprogramowania
- Nie przeskanowano

Status ten może się przydać do filtrowania archiwów kopii zapasowych.



Ograniczenia

- Bezpieczne odzyskiwanie jest obsługiwane w przypadku komputerów fizycznych i maszyn wirtualnych z systemem Windows, na których jest zainstalowany agent ochrony.
- Bezpieczne odzyskiwanie jest obsługiwane w przypadku kopii zapasowych typu **Cały komputer** i **Dyski/woluminy**.
- Skanowanie pod kątem złośliwego oprogramowania jest wykonywane tylko w odniesieniu do woluminów NTFS. Woluminy z innym systemem plików niż NTFS są odzyskiwane bez skanowania antywirusowego.
- Bezpieczne odzyskiwanie nie jest obsługiwane w przypadku kopii zapasowych utworzonych przy użyciu funkcji Ciągła ochrona danych (Continuous data protection, CDP) przechowywanych w archiwum. Aby odzyskać dane z kopii zapasowej CDP, uruchom dodatkową operację odzyskiwania przy użyciu opcji **Pliki/foldery**. Dodatkowe informacje na temat kopii zapasowych CDP można znaleźć w sekcji "Ciągła ochrona danych" (s. 437).

© Acronis International GmbH, 2003-2024

Odzyskiwanie komputera

Odzyskiwanie komputerów fizycznych

W tej sekcji opisano odzyskiwanie komputerów fizycznych przy użyciu interfejsu internetowego.

Czasem lepiej użyć nośnika startowego, a nie interfejsu internetowego. Dotyczy to odzyskiwania następujących elementów:

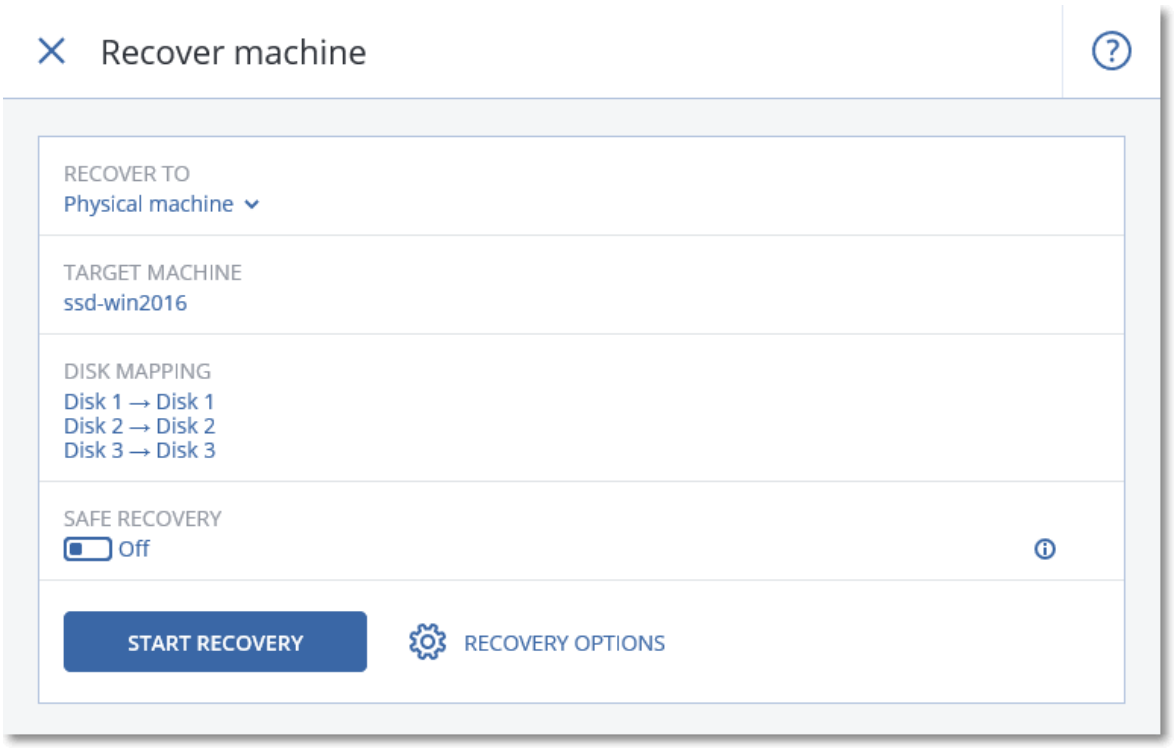
- Komputer z systemem macOS
- Komputer z obszaru dzierżawcy w trybie zgodności
- Dowolny system operacyjny na komputer bez systemu operacyjnego lub komputer w trybie offline
- Struktura woluminów logicznych (woluminy utworzone przez narzędzie Logical Volume Manager w systemie Linux). Nośnik umożliwia automatyczne odtworzenie struktury woluminu logicznego.

Uwaga
Nie można odzyskać kopii zapasowych na poziomie dysku z komputerów Mac z procesorami Intel na komputery Mac z procesorami Apple Silicon i na odwrót. Można odzyskać pliki i foldery.

Aby odzyskać komputer fizyczny

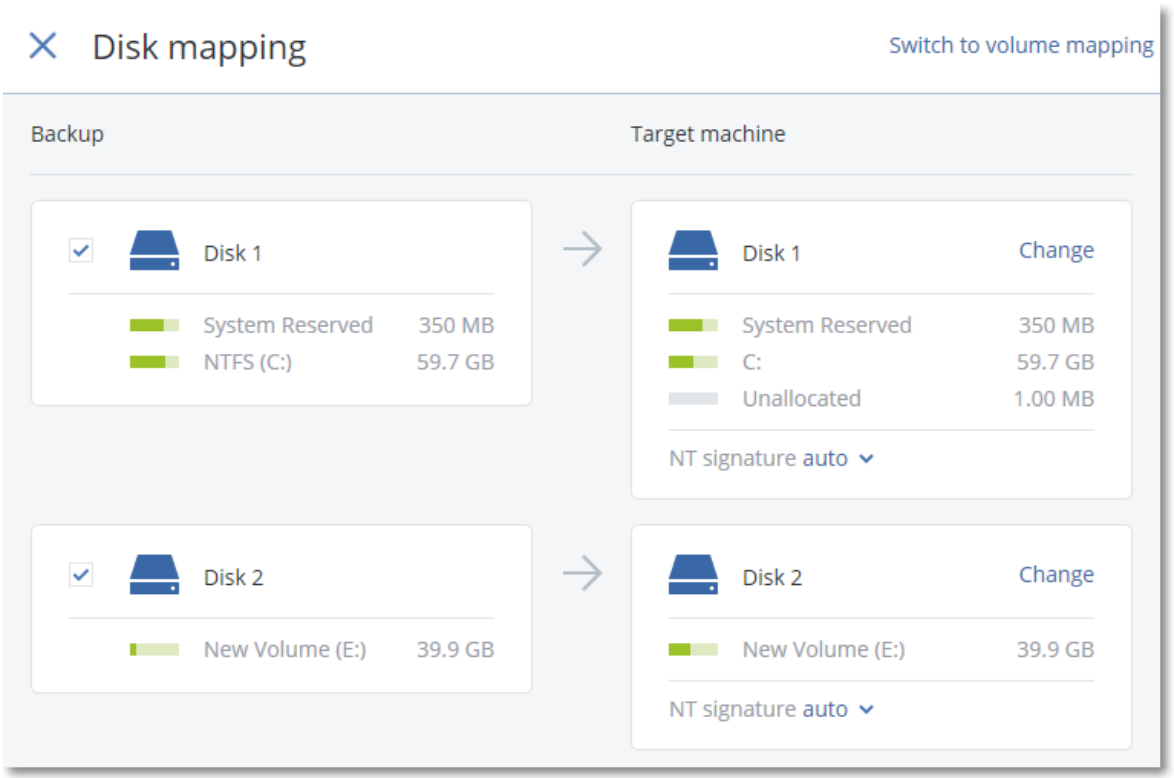
1. Wybierz komputer uwzględniony w kopii zapasowej.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji. Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub współdzielony magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer docelowy będący w trybie online i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.
   - Odzyskaj komputer zgodnie z instrukcjami podanymi w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego”.
4. Kliknij **Odzyskaj** > **Cały komputer**.
   Program automatycznie zamapuje dyski z kopii zapasowej na dyski komputera docelowego.
   Aby odzyskać na inny komputer fizyczny, kliknij **Komputer docelowy** i wybierz komputer docelowy będący w trybie online.

© Acronis International GmbH, 2003-2024



5. Jeśli mapowanie dysku się nie powiedzie lub będzie niezgodne z oczekiwaniami, kliknij **Mapowanie woluminów**, aby zamapować dyski ręcznie.

   Sekcja mapowania umożliwia też wybranie poszczególnych dysków lub woluminów do odzyskania. Możesz przełączać się między dyskami i woluminami do odzyskania przy użyciu linku **Przełącz na...** w prawym górnym rogu.



© Acronis International GmbH, 2003-2024

6. [Możliwość dostępna tylko w przypadku komputerów z systemem Windows, na których jest zainstalowany agent ochrony] Włącz przełącznik **Bezpieczne odzyskiwanie**, aby mieć pewność, że odzyskane dane będą wolne od złośliwego oprogramowania. Dodatkowe informacje na temat działania bezpiecznego odzyskiwania można znaleźć w sekcji "Bezpieczne odzyskiwanie" (s. 535).
7. Kliknij **Rozpocznij odzyskiwanie**.
8. Potwierdź, że chcesz zastąpić dyski ich wersjami z kopii zapasowej. Określ, czy komputer ma zostać automatycznie ponownie uruchomiony.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Komputer fizyczny na maszynę wirtualną

Możesz odzyskać komputer fizyczny na maszynę wirtualną na jednym z obsługiwanych hiperwizorów. Metody tej można również użyć do migracji komputera fizycznego na maszynę wirtualną. Więcej informacji na temat obsługiwanych ścieżek migracji komputera fizycznego na maszynę wirtualną (P2V) można znaleźć w sekcji „Migracja komputera”.

W tej sekcji opisano odzyskiwanie komputera fizycznego jako maszyny wirtualnej przy użyciu interfejsu internetowego. Operację tę można wykonać, jeśli jest zainstalowany co najmniej jeden agent dla odpowiedniego hiperwizora i został on zarejestrowany na serwerze Acronis Management Server. Na przykład odzyskanie na host VMware ESXi wymaga co najmniej jednego agenta dla VMware zainstalowanego i zarejestrowanego w środowisku, a odzyskanie na host Hyper-V — co najmniej jednego agenta dla Hyper-V.

Odzyskiwanie przy użyciu interfejsu internetowego nie jest dostępne w przypadku dzierżawców w trybie zgodności.

Uwaga
Nie można odzyskiwać maszyn wirtualnych macOS na hosty Hyper-V, ponieważ funkcja Hyper-V nie obsługuje systemu macOS. Maszyny wirtualne macOS można odzyskiwać na host VMware zainstalowany na sprzęcie Mac.

Ponadto nie można odzyskiwać kopii zapasowych komputerów fizycznych z systemem macOS jako maszyn wirtualnych.

Aby odzyskać komputer fizyczny jako maszynę wirtualną

1. Wybierz komputer uwzględniony w kopii zapasowej.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji. Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer będący w trybie online i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

© Acronis International GmbH, 2003-2024

- Odzyskaj komputer zgodnie z instrukcjami podanymi w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego”.

4. Kliknij **Odzyskaj** > **Cały komputer**.
5. W polu **Odzyskaj do** wybierz **Maszyna wirtualna**.
6. Kliknij **Komputer docelowy**.
   a. Wybierz hiperwizor.

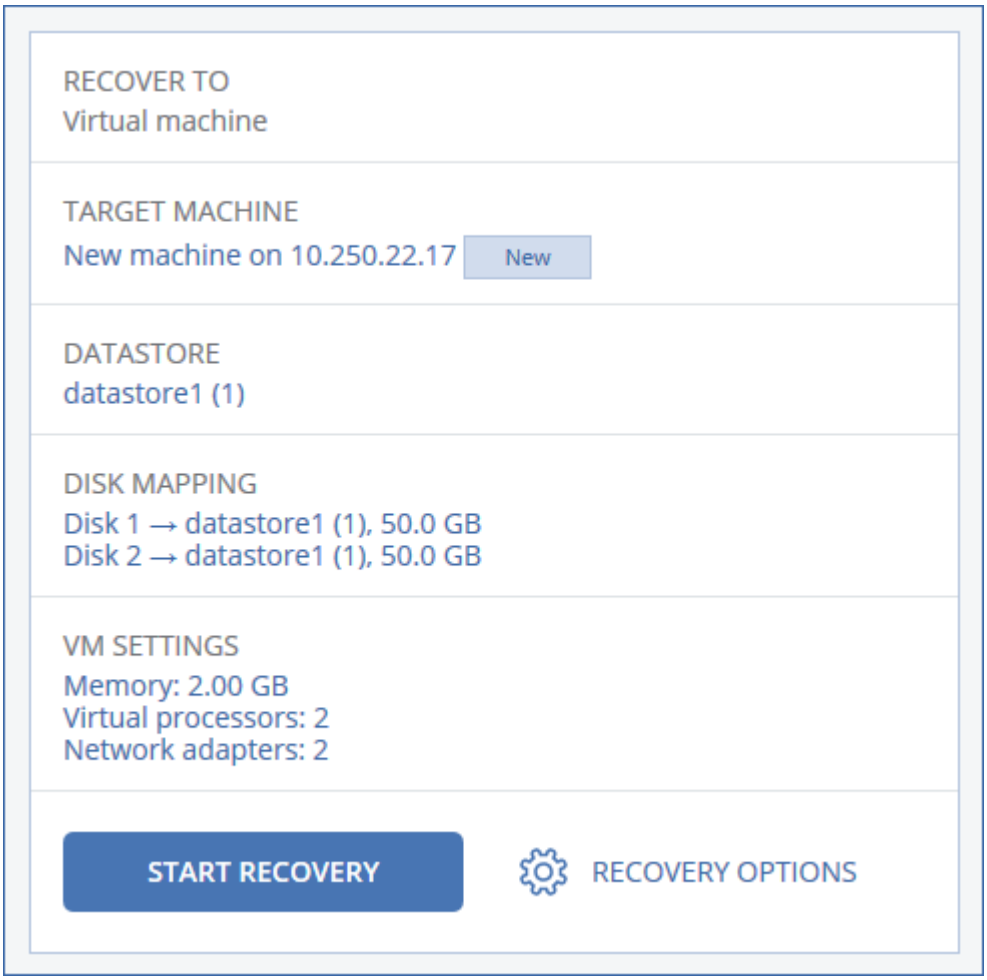
   Uwaga
   Musi być zainstalowany co najmniej jeden agent dla danego hiperwizora i zarejestrowany na serwerze Acronis Management Server.

   b. Określ, czy chcesz odzyskać na nową, czy na już istniejącą maszyną wirtualną. Lepsza jest opcja nowej maszyny, ponieważ nie wymaga, aby konfiguracja dysków maszyny docelowej była dokładnie taka sama jak konfiguracja dysków w kopii zapasowej.
   c. Wybierz host i określ nazwę nowej maszyny lub wybierz istniejącą maszynę docelową.
   d. Kliknij **OK**.
7. [W przypadku środowiska Virtuozzo Hybrid Infrastructure] Kliknij **Ustawienia maszyny wirtualnej** i wybierz **Wariant**. Opcjonalnie można zmienić rozmiar pamięci, liczbę procesorów oraz połączenia sieciowe maszyny wirtualnej.

   Uwaga
   Wybranie wariantu jest wymagane w przypadku środowiska Virtuozzo Hybrid Infrastructure.

8. [Opcjonalnie] Skonfiguruj dodatkowe opcje odzyskiwania:
   - [Opcja niedostępna w przypadku środowiska Virtuozzo Hybrid Infrastructure] Kliknij **Magazyn danych** w przypadku hosta ESXi lub **Ścieżka** w przypadku hosta Hyper-V, a następnie wybierz magazyn danych (pamięć masową) dla maszyny wirtualnej.
   - Kliknij **Mapowanie dysków**, aby wybrać magazyn danych (pamięć masową), interfejs i tryb alokowania dla każdego dysku wirtualnego. Sekcja mapowania umożliwia też wybranie poszczególnych dysków do odzyskania.
     W przypadku środowiska Virtuozzo Hybrid Infrastructure możesz tylko wybrać zasady magazynowania dla dysków docelowych. W tym celu zaznacz żądany dysk docelowy, a następnie kliknij Zmień. W otwartym bloku kliknij ikonę koła zębatego, zaznacz zasady magazynowania, a następnie kliknij Gotowe.
   - [W przypadku środowisk VMware ESXi, Hyper-V i Red Hat Virtualization / oVirt] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów i połączenia sieciowe maszyny wirtualnej.

© Acronis International GmbH, 2003-2024



9. [Możliwość dostępna tylko w przypadku komputerów z systemem Windows, na których jest zainstalowany agent ochrony] Włącz przełącznik **Bezpieczne odzyskiwanie**, aby mieć pewność, że odzyskane dane będą wolne od złośliwego oprogramowania. Dodatkowe informacje na temat działania bezpiecznego odzyskiwania można znaleźć w sekcji "Bezpieczne odzyskiwanie" (s. 535).
10. Kliknij **Rozpocznij odzyskiwanie**.
11. W przypadku odzyskiwania na istniejącą maszynę wirtualną potwierdź, że chcesz zastąpić dyski.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Odzyskiwanie maszyny wirtualnej

Istnieje możliwość odzyskiwania maszyn wirtualnych z ich kopii zapasowych.

Uwaga
W przypadku dzierżawców w trybie zgodności nie można odzyskiwać kopii zapasowych w konsoli Cyber Protect. Więcej informacji na temat odzyskiwania takich kopii zapasowych można znaleźć w sekcji "Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności" (s. 1182).

Wymagania wstępne

© Acronis International GmbH, 2003-2024

- Podczas odzyskiwania maszyna wirtualna nie może działać. Domyślnie oprogramowanie zatrzyma maszynę bez wyświetlenia monitu. Po zakończeniu odzyskiwania trzeba będzie ręcznie uruchomić maszynę. To domyślne zachowanie można zmienić za pomocą opcji odzyskiwania służącej do zarządzania zasilaniem maszyn wirtualnych (kliknij **Opcje odzyskiwania** > **Zarządzanie zasilaniem maszyn wirtualnych**).

Procedura

1. Wykonaj jedną z następujących czynności:
   - Wybierz komputer uwzględniony w kopii zapasowej, kliknij **Odzyskaj**, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.
2. Kliknij **Odzyskaj** > **Cały komputer**.
3. Jeśli chcesz odzyskać na komputer fizyczny, wybierz **Komputer fizyczny** w polu **Odzyskaj do**. W przeciwnym razie pomiń ten krok.

   Odzyskanie na komputer fizyczny jest możliwe pod warunkiem, że konfiguracja dysków komputera docelowego jest dokładnie taka sama jak konfiguracja dysków w kopii zapasowej.

   W takim przypadku przejdź do kroku 4 w sekcji „Komputer fizyczny". W przeciwnym razie zalecamy przeprowadzenie migracji maszyny wirtualnej na komputer fizyczny (V2P) przy użyciu nośnika startowego.
4. [Opcjonalnie] Domyślnie program automatycznie wybierze pierwotny komputer jako komputer docelowy. Aby odzyskać na inną maszynę wirtualną, kliknij **Komputer docelowy**, a następnie wykonaj poniższe czynności:
   a. Wybierz hiperwizor (**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3** lub **oVirt**).

      Do środowiska Virtuozzo można odzyskać tylko maszyny wirtualne Virtuozzo. Więcej informacji na temat migracji maszyny wirtualnej na maszynę wirtualną (V2V) można znaleźć w sekcji „Migracja komputera".

   b. Określ, czy chcesz odzyskać na nową, czy na już istniejącą maszyną wirtualną.

   c. Wybierz host i określ nazwę nowej maszyny lub wybierz istniejącą maszynę docelową.

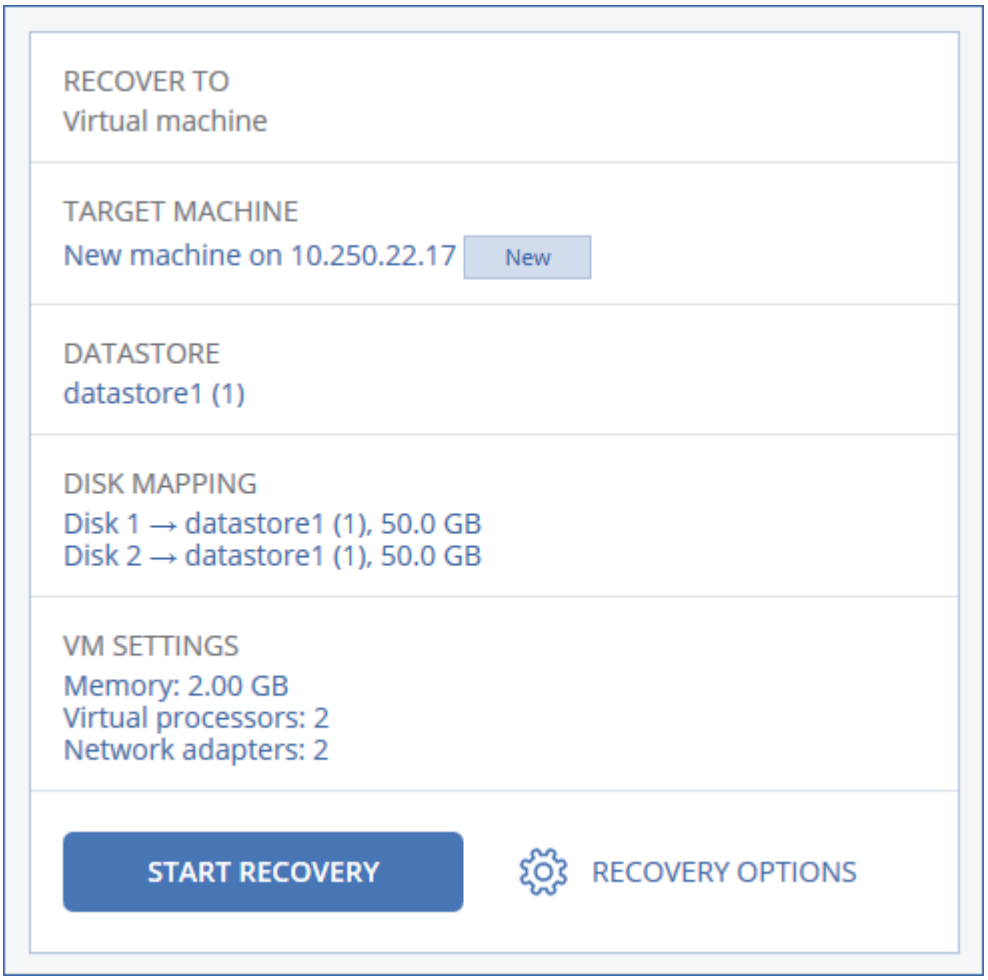
   d. Kliknij **OK**.
5. Skonfiguruj dodatkowe potrzebne opcje odzyskiwania.
   - [Opcjonalnie] [Możliwość niedostępna w przypadku środowisk Virtuozzo Hybrid Infrastructure i Scale Computing HC3] Aby wybrać magazyn danych dla maszyny wirtualnej, kliknij pozycję **Magazyn danych** w przypadku środowiska ESXi, **Ścieżka** w przypadku środowiska Hyper-V lub Virtuozzo lub **Domena magazynu** w przypadku środowiska Red Hat Virtualization (oVirt), a następnie wybierz magazyn danych (pamięć masową) dla maszyny wirtualnej.
   - [Opcjonalnie] Aby wyświetlić magazyn danych (pamięć masową), interfejs i tryb alokowania dla każdego dysku wirtualnego, kliknij **Mapowanie dysków**. Możesz te ustawienia zmienić, chyba że odzyskujesz kontener Virtuozzo lub maszynę wirtualną Virtuozzo Hybrid Infrastructure.

© Acronis International GmbH, 2003-2024

W przypadku środowiska Virtuozzo Hybrid Infrastructure możesz tylko wybrać zasady magazynowania dla dysków docelowych. W tym celu zaznacz żądany dysk docelowy, a następnie kliknij **Zmień**. W otwartym bloku kliknij ikonę koła zębatego, zaznacz zasady magazynowania, a następnie kliknij **Gotowe**.

Sekcja mapowania umożliwia też wybranie poszczególnych dysków do odzyskania.

- [Opcjonalnie] [Dostępne w przypadku platform VMware ESXi, Hyper-V i Virtuozzo] Aby zmienić rozmiar pamięci, liczbę procesorów i połączenia sieciowe maszyny wirtualnej, kliknij **Ustawienia maszyny wirtualnej**.
- [W przypadku środowiska Virtuozzo Hybrid Infrastructure] Aby zmienić rozmiar pamięci i liczbę procesorów maszyny wirtualnej, wybierz **Wariant**.



6. [Możliwość dostępna tylko w przypadku komputerów z systemem Windows, na których jest zainstalowany agent ochrony] Włącz przełącznik **Bezpieczne odzyskiwanie**, aby mieć pewność, że odzyskane dane będą wolne od złośliwego oprogramowania. Dodatkowe informacje na temat działania bezpiecznego odzyskiwania można znaleźć w sekcji "Bezpieczne odzyskiwanie" (s. 535).
7. Kliknij **Rozpocznij odzyskiwanie**.
8. W przypadku odzyskiwania na istniejącą maszynę wirtualną potwierdź, że chcesz zastąpić dyski.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

© Acronis International GmbH, 2003-2024

Odzyskiwanie z ponownym uruchomieniem

Odzyskiwanie po ponownym uruchomieniu jest obsługiwane na komputerach z systemem Windows i Linux.

Możesz wybrać, czy komputer ma zostać automatycznie uruchomiony ponownie, czy ma mu zostać przypisany status **Wymagana interakcja**. Odzyskany system operacyjny automatycznie przechodzi w tryb online.

Ponowne uruchomienie jest wymagane w przypadku odzyskiwania następujących elementów:

- System operacyjny
  Na przykład w przypadku odzyskiwania całego komputera lub woluminu systemowego komputera.
- Zaszyfrowane woluminy
  Na przykład w przypadku odzyskiwania woluminów zaszyfrowanych za pomocą funkcji BitLocker lub CheckPoint.

Ważne
Zaszyfrowane woluminy z kopii zapasowej są odzyskiwane jako niezaszyfrowane.

Na odzyskanym komputerze automatycznie przygotowywane jest środowisko odzyskiwania. Gdy środowisko będzie gotowe, komputer zostanie uruchomiony ponownie, a następnie zostanie otwarte środowisko odzyskiwania. Po zakończeniu odzyskiwania zostanie uruchomiony system operacyjny.

Środowisko odzyskiwania

Odzyskiwanie z ponownym uruchomieniem wykorzystuje środowisko odzyskiwania systemu Linux.

Uwaga
Odzyskanie komputera z zaszyfrowanym woluminem systemowym wymaga co najmniej jednego niezaszyfrowanego woluminu na tym samym komputerze.

Wymagania dotyczące miejsca na dysku

Środowisko odzyskiwania wymaga miejsca na dysku na pliki tymczasowe. Wymagania różnią się w zależności od odzyskiwanego komputera.

W poniższej tabeli zestawiono dostępne opcje.

Tryb startowy	Komputer z niezaszyfrowanym woluminem systemowym	Komputer z zaszyfrowanym woluminem systemowym
BIOS	200 MB na woluminie systemowym	400 MB na woluminie niezaszyfrowanym
UEFI	200 MB na partycji systemowej EFI (ESP)	Jedna z następujących możliwości:

© Acronis International GmbH, 2003-2024

Tryb startowy	Komputer z niezaszyfrowanym woluminem systemowym	Komputer z zaszyfrowanym woluminem systemowym
		• 400 MB na partycji systemowej EFI (ESP) • 200 MB na partycji systemowej EFI (ESP) i 200 MB na partycji niezaszyfrowanej dostępnej podczas procesu uruchamiania

Ograniczenia

- Przed przystąpieniem do odzyskiwania należy zablokować wszystkie zaszyfrowane woluminy niesystemowe. Wolumin można zablokować przez otwarcie znajdującego się na nim pliku. Jeśli wolumin nie zostanie zablokowany, odzyskiwanie będzie kontynuowane bez ponownego uruchomienia, a wolumin może nie zostać rozpoznany przez system operacyjny.

  Nie trzeba blokować zaszyfrowanego woluminu systemowego.

Rozwiązywanie problemów

Jeśli odzyskiwanie się nie powiedzie i po ponownym uruchomieniu pojawi się komunikat `Nie można uzyskać pliku z partycji`, wyłącz funkcję Secure Boot. Aby uzyskać więcej informacji, zobacz sekcję Disabling Secure Boot (Wyłączanie funkcji Secure Boot) w dokumentacji firmy Microsoft.

Odzyskiwanie dysków przy użyciu nośnika startowego

Informacje na temat tworzenia nośnika startowego można znaleźć w sekcji "Tworzenie fizycznego nośnika startowego" (s. 761).

Uwaga
Nie można odzyskać kopii zapasowych na poziomie dysku z komputerów Mac z procesorami Intel na komputery Mac z procesorami Apple Silicon i na odwrót. Można odzyskać pliki i foldery.

Aby odzyskać dyski przy użyciu nośnika startowego

1. Uruchom komputer docelowy, korzystając z nośnika startowego.
2. [Tylko w przypadku odzyskiwania komputera Mac] W przypadku odzyskiwania dysków/woluminów sformatowanych przy użyciu systemu plików APFS na inny komputer niż pierwotny lub komputer bez systemu operacyjnego, należy ręcznie odtworzyć oryginalną konfigurację dysków:
   a. Kliknij **Narzędzie dyskowe**.
   b. Wymaż dane z dysku docelowego i sformatuj go z zastosowaniem systemu plików APFS. Instrukcje można znaleźć w artykule https://support.apple.com/en-us/HT208496#erasedisk.
   c. Odtwórz oryginalną konfigurację dysków. Instrukcje można znaleźć w artykule https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-

© Acronis International GmbH, 2003-2024

dskua9e6a110/19.0/mac/10.15.

d. Kliknij **Narzędzie dyskowe** > **Zamknij Narzędzie dyskowe**.

3. Kliknij **Zarządzaj tym komputerem lokalnie** lub kliknij **Ratunkowy nośnik startowy** dwa razy, w zależności od typu używanego nośnika.
4. Jeśli w danej sieci jest włączony serwer proxy, kliknij **Narzędzia** > **Serwer proxy**, a następnie podaj nazwę hosta / adres IP, port i poświadczenia serwera proxy. W przeciwnym razie pomiń ten krok.
5. [Opcjonalnie] W przypadku odzyskiwania systemu Windows lub Linux kliknij **Narzędzia** > **Zarejestruj nośnik w usłudze Cyber Protection**, a następnie wybierz token rejestracji uzyskany podczas pobierania nośnika. Jeśli wykonasz tę czynność, nie będzie już konieczne wprowadzanie poświadczeń lub kodu rejestracji, aby uzyskać dostęp do magazynu chmurowego, tak jak opisano w kroku 8.
6. Na ekranie powitalnym kliknij **Odzyskaj**.
7. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
8. Określ lokalizację kopii zapasowej:
   - Aby odzyskać z chmury, wybierz **Chmura**. Wprowadź poświadczenia konta, do którego jest przypisany komputer uwzględniony w kopii zapasowej.

     W przypadku odzyskiwania systemu operacyjnego Windows lub Linux można zażądać kodu rejestracji, aby wykorzystać go zamiast poświadczeń. Kliknij **Użyj kodu rejestracji** > **Zażądaj kodu**. W programie zostanie wyświetlone łącze oraz kod rejestracji. Możesz je skopiować i dokonać rejestracji na innym komputerze. Kod rejestracji jest ważny przez godzinę.
   - Aby odzyskać z folderu lokalnego lub sieciowego, przejdź do niego w obszarze **Foldery lokalne** lub **Foldery sieciowe**.
   - Aby odzyskać dane z lokalizacji kopii zapasowych w chmurze publicznej, takiej jak Microsoft Azure, Amazon S3, Wasabi czy platformy zgodne z S3, najpierw kliknij **Zarejestruj nośnik w usłudze Cyber Protection**, a następnie skonfiguruj odzyskiwanie za pomocą interfejsu internetowego. Więcej informacji na temat zdalnego zarządzania multimediami za pośrednictwem interfejsu internetowego można znaleźć w sekcji "Operacje zdalne dotyczące nośnika startowego" (s. 779).

   Kliknij **OK**, aby zatwierdzić wybór.
9. Wybierz kopię zapasową, z której chcesz odzyskać dane. Jeśli pojawi się monit, wpisz hasło kopii zapasowej.
10. W polu **Zawartość kopii zapasowej** wybierz dyski, które chcesz odzyskać. Kliknij **OK**, aby zatwierdzić wybór.
11. W obszarze **Lokalizacja odzyskiwania** oprogramowanie automatycznie zamapuje wybrane dyski na dyski docelowe.

    Jeśli mapowanie się nie powiedzie lub będzie niezgodne z oczekiwaniami, należy zamapować dyski ręcznie.

© Acronis International GmbH, 2003-2024

Uwaga
Zmiana układu dysków może uniemożliwić uruchomienie systemu operacyjnego. Najlepiej użyć układu dysków pierwotnego komputera, chyba że ma się pewność udanej operacji.

12. [W przypadku odzyskiwania systemu Linux] Jeśli komputer uwzględniony w kopii zapasowej ma woluminy logiczne i chcesz odtworzyć ich pierwotną strukturę:
    a. Upewnij się, że liczba i pojemność dysków w komputerze docelowym są takie same lub większe niż liczba i pojemność dysków w pierwotnym komputerze, a następnie kliknij **Zastosuj RAID/LVM**.
    b. Zapoznaj się ze strukturą woluminów, a następnie utwórz ją, klikając **Zastosuj RAID/LVM**.
13. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby określić dodatkowe ustawienia.
14. Kliknij **OK**, aby rozpocząć odzyskiwanie.

Używanie funkcji Universal Restore

Najnowsze systemy operacyjne można uruchamiać po odzyskaniu w innej konfiguracji sprzętowej, w tym na platformach VMware bądź Hyper-V. Jeśli odzyskany system operacyjny się nie uruchamia, należy za pomocą narzędzia Universal Restore zaktualizować sterowniki i moduły, które mają zasadnicze znaczenie dla uruchamiania systemu operacyjnego.

Narzędzie Universal Restore można stosować w odniesieniu do systemów Windows oraz Linux.

Aby zastosować narzędzie Universal Restore

1. Uruchom komputer za pomocą nośnika startowego.
2. Kliknij **Zastosuj funkcję Universal Restore**.
3. Jeśli na komputerze jest więcej niż jeden system operacyjny, wybierz ten z nich, w którym chcesz zastosować narzędzie Universal Restore.
4. [Tylko w systemie Windows] Skonfiguruj dodatkowe ustawienia.
5. Kliknij **OK**.

Narzędzie Universal Restore w systemie Windows

Przygotowanie

Przygotuj sterowniki

Przed zastosowaniem narzędzia Universal Restore w systemie operacyjnym Windows sprawdź, czy masz sterowniki dla nowego kontrolera dysku twardego i chipsetu. Te sterowniki mają zasadnicze znaczenie dla uruchamiania systemu operacyjnego. Użyj płyty CD lub DVD dostarczonej przez dostawcę sprzętu lub pobierz sterowniki z witryny internetowej dostawcy. Pliki sterowników powinny mieć rozszerzenie *.inf. Jeśli pobrano sterowniki w formacie exe, cab lub zip, trzeba je wyodrębnić za pomocą aplikacji innej firmy.

© Acronis International GmbH, 2003-2024

Sprawdzoną praktyką jest przechowywanie sterowników dla całego sprzętu używanego w organizacji w jednym repozytorium, posortowanym według typu urządzenia lub według konfiguracji sprzętu. Kopię tego repozytorium można przechowywać na płycie DVD lub dysku flash, a wybrane z niego sterowniki można umieścić na nośniku startowym, tworząc niestandardowy nośnik startowy zawierający niezbędne sterowniki (oraz niezbędną konfigurację sieciową) dla każdego z używanych serwerów. Można także po prostu określać ścieżkę do repozytorium za każdym razem, gdy używane jest narzędzie Universal Restore.

Sprawdź dostęp do sterowników w środowisku startowym

Upewnij się, że masz dostęp do urządzenia ze sterownikami podczas pracy z nośnikiem startowym. Użyj nośnika opartego na środowisku WinPE, jeśli urządzenie jest dostępne w systemie Windows, ale nie wykrywa go nośnik oparty na systemie Linux.

Ustawienia narzędzia Universal Restore

Automatyczne wyszukiwanie sterowników

Określ miejsce, w którym program będzie wyszukiwać sterowników warstwy abstrakcji sprzętu (HAL), kontrolera dysku twardego i adapterów sieciowych:

- Jeśli sterowniki znajdują się na płycie lub innym nośniku wymiennym udostępnionym przez dostawcę, włącz opcję **Przeszukaj nośnik wymienny**.
- Jeśli sterowniki znajdują się w folderze sieciowym lub na nośniku startowym, określ ścieżkę do tego folderu, klikając **Dodaj folder**.

Oprócz tego narzędzie Universal Restore przeszuka domyślny folder magazynu sterowników Windows. Jego lokalizacja jest ustalona za pomocą wartości rejestru **DevicePath**, która znajduje się w kluczu rejestru **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Zazwyczaj jest to folder WINDOWS/inf.

Narzędzie Universal Restore przeprowadzi rekurencyjne wyszukiwanie we wszystkich podfolderach określonego folderu, znajdzie najbardziej odpowiednie sterowniki warstwy abstrakcji sprzętu (HAL) i kontrolera dysku twardego spośród dostępnych, a następnie zainstaluje je w systemie. Narzędzie Universal Restore wyszukuje także sterownik adaptera sieciowego, a ścieżka do znalezionego sterownika jest przez nie następnie przekazywana do systemu operacyjnego. Jeśli komputer jest wyposażony w kilka kart interfejsu sieciowego, narzędzie Universal Restore próbuje skonfigurować sterowniki wszystkich kart.

Sterowniki pamięci masowej do zainstalowania mimo to

Ustawienie to jest niezbędne, gdy:

- Komputer jest wyposażony w określony kontroler pamięci masowej, taki jak adapter RAID (w szczególności NVIDIA RAID) lub Fibre Channel.

© Acronis International GmbH, 2003-2024

- Przeprowadzona została migracja do maszyny wirtualnej, w której używany jest kontroler dysku twardego SCSI. Należy korzystać ze sterowników SCSI dołączonych do oprogramowania do wirtualizacji lub pobrać najnowsze wersje sterowników z witryny internetowej producenta oprogramowania.
- Jeśli automatyczne wyszukiwanie sterowników nie ułatwia uruchomienia systemu.

Wskaż odpowiednie sterowniki, klikając **Dodaj sterownik**. Zdefiniowane tutaj sterowniki zostaną zainstalowane, z odpowiednimi ostrzeżeniami, nawet gdy program znajdzie lepsze.

Działanie narzędzia Universal Restore

Po określeniu wymaganych ustawień kliknij **OK**.

Jeśli narzędzie Universal Restore nie znajdzie kompatybilnego sterownika w określonych lokalizacjach, wyświetli monit informujący o problemie z urządzeniem. Wykonaj jedną z następujących czynności:

- Dodaj sterownik do dowolnej ze wskazanych wcześniej lokalizacji i kliknij **Spróbuj ponownie**.
- Jeżeli nie pamiętasz lokalizacji, kliknij **Ignoruj**, aby kontynuować proces. Jeśli wynik będzie niezadowalający, ponownie zastosuj narzędzie Universal Restore. Podczas konfigurowania operacji określ niezbędny sterownik.

Po uruchomieniu system Windows zainicjuje standardową procedurę instalowania nowego sprzętu. Sterownik adaptera sieciowego zostanie zainstalowany dyskretnie, jeśli posiada sygnaturę systemu Microsoft Windows. W przeciwnym razie system Windows poprosi o potwierdzenie zainstalowania niepodpisanego sterownika.

Po wykonaniu tych czynności można skonfigurować połączenie sieciowe i określić sterowniki adaptera wideo, USB oraz innych urządzeń.

Narzędzie Universal Restore w systemie Linux

Narzędzie Universal Restore można stosować w systemach operacyjnych Linux z jądrem w wersji 2.6.8 lub nowszej.

W przypadku zastosowania w systemie operacyjnym Linux narzędzie Universal Restore aktualizuje tymczasowy system plików określany jako początkowy dysk RAM (initrd). Pozwala to na uruchomienia systemu operacyjnego na nowym sprzęcie.

Narzędzie Universal Restore dodaje do początkowego dysku RAM moduły odpowiedzialne za nowy sprzęt (w tym sterowniki urządzeń). Na ogół niezbędne moduły znajdują się w katalogu **/lib/modules**. Gdy narzędzie Universal Restore nie może znaleźć potrzebnego modułu, rejestruje nazwę pliku modułu w dzienniku.

Narzędzie Universal Restore może modyfikować konfigurację programu startowego GRUB. Może to być wymagane na przykład w celu zapewnienia możliwości uruchomienia systemu, gdy układ woluminów na nowym komputerze różni się od układu na komputerze pierwotnym.

Narzędzie Universal Restore nigdy nie modyfikuje jądra systemu Linux.

© Acronis International GmbH, 2003-2024

Przywrócenie oryginalnego początkowego dysku RAM

W razie potrzeby można przywrócić oryginalny początkowy dysk RAM.

Początkowy dysk RAM jest przechowywany w pliku na komputerze. Przed zaktualizowaniem początkowego dysku RAM po raz pierwszy narzędzie Universal Restore zapisuje jego kopię w tym samym katalogu. Nazwą kopii jest nazwa pliku z sufiksem **_acronis_backup.img**. Ta kopia nie zostaje zastąpiona, gdy narzędzie Universal Restore jest uruchamiane więcej niż raz (na przykład po dodaniu brakujących sterowników).

Aby przywrócić oryginalny początkowy dysk RAM, wykonaj dowolną z następujących czynności:

- Zmień odpowiednio nazwę kopii. Wywołaj na przykład polecenie podobne do następującego:

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Określ kopię w wierszu **initrd** konfiguracji programu startowego GRUB.

Odzyskiwanie plików

Odzyskiwanie plików w konsoli Cyber Protect

Uwaga
W przypadku dzierżawców w trybie zgodności nie można odzyskiwać kopii zapasowych w konsoli Cyber Protect. Więcej informacji na temat odzyskiwania takich kopii zapasowych można znaleźć w sekcji "Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności" (s. 1182).

1. Wybierz komputer, który pierwotnie zawierał dane do odzyskania.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
   Jeśli został wybrany komputer fizyczny lub komputer w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:
   - [Zalecane] Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer docelowy będący w trybie online i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.
   - Pobierz pliki z magazynu chmurowego.
   - Użyj nośnika startowego.
4. Kliknij **Odzyskaj** > **Pliki/foldery**.
5. Przejdź do odpowiedniego folderu lub użyj paska wyszukiwania, aby uzyskać listę wymaganych plików i folderów.
   Wyszukiwanie zależy od języka.

© Acronis International GmbH, 2003-2024

Można użyć jednego lub kilku symboli wieloznacznych (* i ?). Więcej informacji na temat stosowania symboli wieloznacznych można znaleźć w sekcji "Maska" (s. 495).

Uwaga
W przypadku kopii zapasowych na poziomie dysku, które są przechowywanie w chmurze, wyszukiwanie jest niedostępne.

6. Wybierz pliki, które chcesz odzyskać.
7. Jeśli chcesz zapisać pliki jako plik .zip, kliknij **Pobierz**, wybierz lokalizację, w której mają zostać zapisane dane, i kliknij **Zapisz**. W przeciwnym razie pomiń ten krok.
   Jeśli wybrane elementy obejmują foldery lub łączny rozmiar wybranych plików przekracza 100 MB, pobieranie jest niedostępne. Aby pobrać większą ilość danych z chmury, skorzystaj z procedury opisanej w sekcji "Pobieranie plików z chmury" (s. 551).
8. Kliknij **Odzyskaj**.
   W polu **Odzyskaj do** kliknij, aby wybrać miejsce docelowe operacji odzyskiwania, lub pozostaw domyślne miejsce docelowe. Domyślne miejsce docelowe różni się w zależności od źródła kopii zapasowej.
   Dostępne są następujące miejsca docelowe:
   - Komputer źródłowy (jeśli jest na nim zainstalowany agent ochrony).
     Jest to komputer, który pierwotnie zawierał pliki do odzyskania.
   - Inne komputery, na których jest zainstalowany agent ochrony — komputery fizyczne, maszyny wirtualne i hosty wirtualizacji, na których jest zainstalowany agent ochrony, lub urządzenia wirtualne.
     Pliki można odzyskać na komputery fizyczne, maszyny wirtualne i hosty wirtualizacji, na których jest zainstalowany agent ochrony. Nie można odzyskać plików na maszyny wirtualne, na których nie ma zainstalowanego agenta ochrony (z wyjątkiem maszyn wirtualnych Virtuozzo).
   - Kontenery lub maszyny wirtualne Virtuozzo.
     Pliki można odzyskać do kontenerów i na maszyny wirtualne Virtuozzo — z pewnymi ograniczeniami. Dodatkowe informacje na ich temat można znaleźć w sekcji "Ograniczenia dotyczące odzyskiwania plików w konsoli Cyber Protect" (s. 555).
9. W polu **Ścieżka** wybierz miejsce docelowe odzyskiwania. Można wybrać jedną z następujących opcji:
   - [W przypadku odzyskiwania na pierwotny komputer] Pierwotna lokalizacja.
   - Folder lokalny na komputerze docelowym lub pamięć masowa lokalnie podłączona do tego komputera.

     Uwaga
     Łącza symboliczne nie są obsługiwane.

   - Folder sieciowy dostępny z komputera docelowego
10. Kliknij **Rozpocznij odzyskiwanie**.

© Acronis International GmbH, 2003-2024

11. Wybierz jedną z następujących opcji zastępowania plików:
    - **Zastąp istniejące pliki**
    - **Zastąp istniejący plik, jeśli jest starszy**
    - **Nie zastępuj istniejących plików**

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Pobieranie plików z chmury

W konsoli Web Restore możesz przeglądać chmurę, wyświetlać zawartość kopii zapasowych i pobierać pliki i foldery uwzględnione w kopiach zapasowych.

Uwaga
Dostęp do konsoli Web Restore możesz uzyskać tylko wtedy, gdy jesteś administratorem klienta Cyber Protection lub użytkownikiem będącym dzierżawcą-klientem. Na poziomie partnera role użytkowników są niedozwolone.

Ograniczenia

- Nie możesz pobierać dysków, woluminów ani całych punktów odzyskiwania uwzględnionych w kopiach zapasowych.
- Podczas przeglądania kopii zapasowych na poziomie dysku woluminy logiczne (takie jak LVM i LDM) nie są wyświetlane.
- Nie możesz przeglądać kopii zapasowych stanu systemu, baz danych SQL ani baz danych programu Exchange.

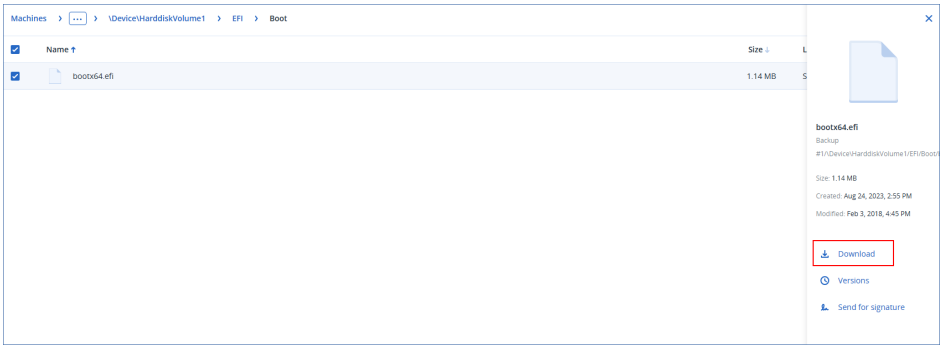
Aby pobrać z chmury pliki i foldery

1. W konsoli Cyber Protection wybierz odpowiednie obciążenie, a następnie kliknij **Odzyskiwanie**.
2. [Jeśli są dostępne różne lokalizacje kopii zapasowych] Wybierz lokalizację kopii zapasowych, a następnie kliknij **Więcej metod odzyskiwania**.
3. Kliknij **Pobierz pliki**.
4. W sekcji **Komputery** kliknij nazwę obciążenia, a następnie kliknij archiwum kopii zapasowych. Archiwum kopii zapasowych zawiera jedną lub więcej kopii zapasowych (punktów odzyskiwania).
5. Kliknij numer kopii zapasowej (punkt odzyskiwania), z której chcesz pobrać pliki lub foldery, a następnie przejdź do wymaganych elementów.
6. Zaznacz pola wyboru obok elementów, które chcesz pobrać.

   Uwaga
   Jeśli wybierzesz wiele elementów, zostaną one pobrane jako plik ZIP.

© Acronis International GmbH, 2003-2024

7. Kliknij **Pobierz**.



Weryfikowanie autentyczności pliku przy użyciu usługi Notary

Jeśli podczas tworzenia kopii zapasowej było włączone poświadczanie, istnieje możliwość weryfikacji autentyczności pliku uwzględnionego w kopii zapasowej.

Aby zweryfikować autentyczność pliku

1. Wybierz plik zgodnie z opisem podanym w krokach 1–6 sekcji „Odzyskiwanie plików przy użyciu interfejsu internetowego" lub w krokach 1–5 sekcji „Pobieranie plików z chmury".
2. Sprawdź, czy wybrany plik jest oznaczony następującą ikoną: . Oznacza to, że plik został notaryzowany.
3. Wykonaj jedną z następujących czynności:
   - Kliknij opcję **Sprawdź**.
     Program sprawdza autentyczność pliku i wyświetla wynik.
   - Kliknij opcję **Uzyskaj certyfikat**.
     Certyfikat potwierdzający notaryzację pliku zostanie otwarty w oknie przeglądarki internetowej. Okno to zawiera również instrukcje umożliwiające ręczną weryfikację autentyczności pliku.

Podpisywanie pliku w usłudze ASign

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Usługa ASign umożliwia wielu osobom elektroniczne podpisanie pliku uwzględnionego w kopii zapasowej. Funkcja ta jest dostępna tylko w przypadku kopii zapasowych na poziomie plików przechowywanych w chmurze.

W danej chwili może być podpisana tylko jedna wersja pliku. Jeśli utworzono wiele kopii zapasowych pliku, należy wybrać wersję do podpisania — tylko ta wersja będzie podpisana.

Usługa ASign umożliwia na przykład podpisywanie elektroniczne następujących plików:

© Acronis International GmbH, 2003-2024

- Umowy wynajmu i dzierżawy
- Umowy sprzedaży
- Umowy zakupu zasobów
- Umowy pożyczek
- Potwierdzenia zgody
- Dokumenty finansowe
- Dokumenty ubezpieczenia
- Zrzeczenia odpowiedzialności
- Dokumenty opieki zdrowotnej
- Prace naukowe
- Certyfikaty autentyczności produktu
- Umowy o zachowaniu poufności
- Listy ofertowe
- Umowy o poufności
- Umowy wykonawców niezależnych

Podpisywanie wersji pliku

1. Wybierz plik zgodnie z opisem podanym w krokach 1–6 sekcji „Odzyskiwanie plików przy użyciu interfejsu internetowego" lub w krokach 1–5 sekcji „Pobieranie plików z chmury".
2. Dopilnuj, aby w lewym panelu została wybrana poprawna data i godzina.
3. Kliknij opcję **Podpisz tę wersję pliku**.
4. Określ hasło do konta w chmurze, na którym jest przechowywana kopia zapasowa. Nazwa logowania konta jest wyświetlana w oknie monitu.
   Interfejs usługi ASign zostanie otwarty w oknie przeglądarki internetowej.
5. Dodaj inne osoby podpisujące, określając ich adresy e-mail. Po wysłaniu zaproszeń nie można dodawać ani usuwać osób podpisujących, więc upewnij się, że lista zawiera wszystkie osoby, których podpis jest wymagany.
6. Kliknij **Zaproś do podpisania**, aby wysłać zaproszenia do wszystkich osób podpisujących.
   Każda osoba podpisująca otrzymuje wiadomość e-mail z prośbą o podpisanie. Gdy plik podpiszą już wszystkie poproszone o to osoby, zostanie on znotaryzowany i podpisany przez usługę notaryzacji.
   Otrzymasz powiadomienia o podpisaniu pliku przez każdą z tych osób oraz o ukończeniu całego procesu. Aby uzyskać dostęp do strony internetowej usługi ASign, kliknij **Wyświetl szczegóły** w dowolnej otrzymanej wiadomości e-mail.
7. Po zakończeniu procesu przejdź do strony internetowej usługi ASign i kliknij **Uzyskaj dokument**, aby pobrać dokument PDF, który zawiera:

© Acronis International GmbH, 2003-2024

- Strona Certyfikat podpisu zawiera zebrane podpisy.
- Strona Ścieżka audytu zawiera historię działań: kiedy zaproszenie zostało wysłane do osób podpisujących, kiedy plik został podpisany przez poszczególne osoby itd.

Odzyskiwanie plików przy użyciu nośnika startowego

Informacje na temat tworzenia nośnika startowego można znaleźć w sekcji „Tworzenie nośnika startowego”.

Aby odzyskać pliki przy użyciu nośnika startowego

1. Uruchom komputer docelowy, korzystając z nośnika startowego.
2. Kliknij **Zarządzaj tym komputerem lokalnie** lub kliknij **Ratunkowy nośnik startowy** dwa razy, w zależności od typu używanego nośnika.
3. Jeśli w danej sieci jest włączony serwer proxy, kliknij **Narzędzia** > **Serwer proxy**, a następnie podaj nazwę hosta / adres IP, port i poświadczenia serwera proxy. W przeciwnym razie pomiń ten krok.
4. [Opcjonalnie] W przypadku odzyskiwania systemu Windows lub Linux kliknij **Narzędzia** > **Zarejestruj nośnik w usłudze Cyber Protection**, a następnie wybierz token rejestracji uzyskany podczas pobierania nośnika. Jeśli wykonasz tę czynność, nie będzie już konieczne wprowadzanie poświadczeń lub kodu rejestracji, aby uzyskać dostęp do magazynu chmurowego, tak jak opisano w kroku 7.
5. Na ekranie powitalnym kliknij **Odzyskaj**.
6. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
7. Określ lokalizację kopii zapasowej:
   - Aby odzyskać z chmury, wybierz **Chmura**. Wprowadź poświadczenia konta, do którego jest przypisany komputer uwzględniony w kopii zapasowej.
     W przypadku odzyskiwania systemu operacyjnego Windows lub Linux można zażądać kodu rejestracji, aby wykorzystać go zamiast poświadczeń. Kliknij **Użyj kodu rejestracji** > **Zażądaj kodu**. W programie zostanie wyświetlone łącze oraz kod rejestracji. Możesz je skopiować i dokonać rejestracji na innym komputerze. Kod rejestracji jest ważny przez godzinę.
   - Aby odzyskać z folderu lokalnego lub sieciowego, przejdź do niego w obszarze **Foldery lokalne** lub **Foldery sieciowe**.
   - Aby odzyskać dane z lokalizacji kopii zapasowych w chmurze publicznej, takiej jak Microsoft Azure, Amazon S3, Wasabi czy platformy zgodne z S3, najpierw kliknij **Zarejestruj nośnik w usłudze Cyber Protection**, a następnie skonfiguruj odzyskiwanie za pomocą interfejsu internetowego. Więcej informacji na temat zdalnego zarządzania multimediami za pośrednictwem interfejsu internetowego można znaleźć w sekcji "Operacje zdalne dotyczące nośnika startowego" (s. 779).

   Kliknij **OK**, aby zatwierdzić wybór.
8. Wybierz kopię zapasową, z której chcesz odzyskać dane. Jeśli pojawi się monit, wpisz hasło kopii zapasowej.

© Acronis International GmbH, 2003-2024

9. W polu **Zawartość kopii zapasowej** wybierz **Foldery/pliki**.
10. Wybierz dane, które chcesz odzyskać. Kliknij **OK**, aby zatwierdzić wybór.
11. W obszarze **Lokalizacja odzyskiwania** określ folder. Opcjonalnie możesz zablokować zastępowanie nowszych wersji plików lub wykluczyć niektóre pliki z odzyskiwania.
12. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby określić dodatkowe ustawienia.
13. Kliknij **OK**, aby rozpocząć odzyskiwanie.

Wyodrębnianie plików z lokalnych kopii zapasowych

Można przeglądać zawartość kopii zapasowych i wyodrębniać potrzebne pliki.

Wymagania

- Ta funkcja jest dostępna tylko w przypadku korzystania z Eksploratora plików w systemie Windows.
- System plików w kopii zapasowej musi być jednym z następujących: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS lub HFS+.

Wymagania wstępne

- Na komputerze używanym do przeglądania kopii zapasowej musi być zainstalowany agent ochrony.
- Kopia zapasowa musi być przechowywana w folderze lokalnym lub udziale sieciowym (SMB/CIFS).

Aby wyodrębnić pliki z kopii zapasowej

1. W Eksploratorze plików przejdź do lokalizacji kopii zapasowej.
2. Kliknij dwukrotnie plik kopii zapasowej. Nazwy plików mają następującą strukturę:
   `<nazwa komputera> – <GUID planu ochrony>`
3. Jeśli kopia zapasowa jest zaszyfrowana, wprowadź hasło szyfrowania. W przeciwnym razie pomiń ten krok.
   W Eksploratorze plików zostaną wyświetlone punkty odzyskiwania.
4. Kliknij dwukrotnie odpowiedni punkt odzyskiwania.
   W Eksploratorze plików zostaną wyświetlone dane z kopii zapasowej.
5. Przejdź do odpowiedniego folderu.
6. Skopiuj potrzebne pliki do dowolnego folderu w systemie plików.

Ograniczenia dotyczące odzyskiwania plików w konsoli Cyber Protect

Dzierżawcy w trybie zgodności

W przypadku dzierżawców w trybie zgodności nie można odzyskiwać kopii zapasowych w konsoli Cyber Protect. Więcej informacji na temat odzyskiwania takich kopii zapasowych można znaleźć w sekcji "Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności" (s. 1182).

© Acronis International GmbH, 2003-2024

Odzyskiwanie do kontenerów Virtuozzo lub maszyn wirtualnych Virtuozzo

- Na docelowej maszynie wirtualnej musi być zainstalowany agent gość QEMU.
- [Dotyczy tylko odzyskiwania do konwerterów] Punkty montowania w kontenerach nie mogą być miejscami docelowymi odzyskiwania. Nie można na przykład odzyskać plików na drugi dysk twardy lub udział NFS zamontowany do kontenera.
- W przypadku odzyskiwania plików na maszynę wirtualną z systemem Windows i włączenia opcji odzyskiwania "Zabezpieczenia na poziomie plików" (s. 562) atrybut bitu archiwum zostaje ustawiony na potrzeby odzyskiwanych plików.
- Pliki ze znakami spoza zestawu ANSI w nazwach są odzyskiwane z nieprawidłowymi nazwami na komputerach z systemem Windows Server 2012 lub starszym oraz komputerach z systemem Windows 7 lub starszym.
- Aby odzyskać pliki na maszynach wirtualnych CentOS lub Red Hat Enterprise Linux, które działają na serwerze hybrydowym Virtuozzo, należy edytować plik `qemu-ga` w sposób następujący:
  - Na docelowej maszynie wirtualnej przejdź do folderu `/etc/sysconfig/` i otwórz plik `qemu-ga` do edycji.
  - Przejdź do następującego wiersza, a następnie usuń wszystko to, co się znajduje po znaku równości (=):

    ```
    BLACKLIST_RPC=
    ```

  - Uruchom ponownie agenta gościa QEMU, uruchamiając następujące polecenie:

    ```
    systemctl restart qemu-guest-agent
    ```

Odzyskiwanie stanu systemu

Uwaga
W przypadku dzierżawców w trybie zgodności nie można odzyskiwać kopii zapasowych w konsoli Cyber Protect. Więcej informacji na temat odzyskiwania takich kopii zapasowych można znaleźć w sekcji "Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności" (s. 1182).

1. Wybierz komputer, którego stan systemu chcesz odzyskać.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania stanu systemu. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj stan systemu**.
5. Potwierdź, że chcesz zastąpić stan systemu jego wersją z kopii zapasowej.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

© Acronis International GmbH, 2003-2024

Odzyskiwanie konfiguracji ESXi

Do odzyskania konfiguracji ESXi potrzebny jest nośnik startowy oparty na systemie Linux. Informacje na temat tworzenia nośnika startowego można znaleźć w sekcji "Tworzenie fizycznego nośnika startowego" (s. 761).

Jeśli odzyskujesz konfigurację ESXi na host inny niż pierwotny, a pierwotny host ESXi jest nadal podłączony do serwera vCenter, rozłącz ten host i usuń go z serwera vCenter, aby uniknąć niespodziewanych problemów podczas odzyskiwania. Jeśli chcesz zachować pierwotny host razem z odzyskanym, możesz go dodać ponownie po zakończeniu operacji odzyskiwania.

Maszyny wirtualne działające na hoście nie są uwzględniane w kopii zapasowej konfiguracji ESXi. Można jednak osobno tworzyć ich kopie zapasowe i osobno je odzyskiwać.

Aby odzyskać konfigurację ESXi

1. Uruchom komputer docelowy, korzystając z nośnika startowego.
2. Kliknij **Zarządzaj tym komputerem lokalnie**.
3. Na ekranie powitalnym kliknij **Odzyskaj**.
4. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
5. Określ lokalizację kopii zapasowej:
   - Przejdź do folderu w obszarze **Foldery lokalne** lub **Foldery sieciowe**.

   Kliknij **OK**, aby zatwierdzić wybór.
6. W polu **Pokaż** wybierz **Konfiguracje ESXi**.
7. Wybierz kopię zapasową, z której chcesz odzyskać dane. Jeśli pojawi się monit, wpisz hasło kopii zapasowej.
8. Kliknij **OK**.
9. W polu **Dyski, które mają zostać wykorzystane na potrzeby nowych magazynów danych** zrób tak:
   - W obszarze **Odzyskaj ESXi na** wybierz dysk, na który zostanie odzyskana konfiguracja hosta. W przypadku odzyskiwania konfiguracji na pierwotny host domyślnie zostaje wybrany dysk oryginalny.
   - [Opcjonalnie] W obszarze **Użyj dla nowych magazynów danych** wybierz dyski, na których zostaną utworzone nowe magazyny danych. Zrób to z rozwagą, ponieważ wszystkie dane zapisane na wybranych dyskach zostaną utracone. Jeśli chcesz zachować maszyny wirtualne w istniejących już magazynach danych, nie wybieraj żadnego dysku.
10. Jeśli nie wybierzesz dysków na potrzeby nowych magazynów danych, w polu **Jak utworzyć nowe magazyny danych** wybierz metodę utworzenia magazynów danych: **Utwórz jeden magazyn danych na dysk** lub **Utwórz jeden magazyn danych na wszystkich wybranych dyskach twardych**.
11. [Opcjonalnie] W polu **Mapowanie sieci** zmień wynik automatycznego mapowania przełączników wirtualnych dostępnych w kopii zapasowej na fizyczne karty sieciowe.

© Acronis International GmbH, 2003-2024

12. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby określić dodatkowe ustawienia.
13. Kliknij **OK**, aby rozpocząć odzyskiwanie.

Opcje odzyskiwania

Aby zmodyfikować opcje odzyskiwania, kliknij **Opcje odzyskiwania** podczas konfigurowania odzyskiwania.

Dostępne opcje odzyskiwania

Zakres dostępnych opcji odzyskiwania zależy od następujących czynników:

- Środowisko działania agenta wykonującego operację odzyskiwania (Windows, Linux, macOS lub nośnik startowy)
- Typ odzyskiwanych danych (dyski, pliki, maszyny wirtualne, dane aplikacji)

W poniższej tabeli zestawiono dostępność opcji odzyskiwania.

	Dyski			**Pliki**				**Maszyny wirtualne**	**SQL oraz Exchange**
	Windows	**Linux**	**Nośnik startowy**	**Windows**	**Linux**	**macOS**	**Nośnik startowy**	**ESXi, Hyper-V i Virtuozzo**	**Windows**
Sprawdzanie poprawności kopii zapasowej	+	+	+	+	+	+	+	+	+
Tryb startowy	+	-	-	-	-	-	-	+	-
Data i godzina plików	-	-	-	+	+	+	+	-	-
Obsługa błędów	+	+	+	+	+	+	+	+	+
Wykluczenia plików	-	-	-	+	+	+	+	-	-
Zabezpieczenia na poziomie plików	-	-	-	+	-	-	-	-	-
Flashback	+	+	+	-	-	-	-	+	-
Odzyskiwanie pełnej ścieżki	-	-	-	+	+	+	+	-	-
Punkty	-	-	-	+	-	-	-	-	-

© Acronis International GmbH, 2003-2024

zamontowania									
Wydajność	+	+	-	+	+	+	-	+	+
Polecenia poprzedzające/następujące	+	+	-	+	+	+	-	+	+
Zmiana identyfikatorów SID	+	-	-	-	-	-	-	-	-
Zarządzanie zasilaniem maszyn wirtualnych	-	-	-	-	-	-	-	+	-
Dziennik zdarzeń systemu Windows	+	-	-	+	-	-	-	Tylko Hyper-V	+

Sprawdzanie poprawności kopii zapasowej

Opcja określa, czy przed odzyskaniem danych z kopii zapasowej należy sprawdzić jej poprawność. Dzięki temu można się upewnić, że kopia zapasowa nie jest uszkodzona. Ta operacja jest wykonywana przez agenta ochrony.

Ustawienie wstępne: **Wyłączono**.

Dodatkowe informacje na temat sprawdzania poprawności metodą weryfikacji sumy kontrolnej można znaleźć w sekcji "Weryfikacja sumy kontrolnej" (s. 238).

Uwaga
W zależności od ustawień wybranych przez dostawcę usług sprawdzanie poprawności może być niedostępne w przypadku tworzenia kopii zapasowej w chmurze.

Tryb startowy

Ta opcja jest dostępna tylko w przypadku odzyskiwania komputera fizycznego lub maszyny wirtualnej z kopii zapasowej na poziomie dysku zawierającej system operacyjny Windows.

Opcja umożliwia wybranie trybu startowego (BIOS lub UEFI), którego system Windows użyje po zakończeniu operacji odzyskiwania. Jeśli tryb startowy pierwotnego komputera był inny od wybranego trybu startowego, oprogramowanie:

- Zainicjuje dysk, na który odzyskujesz wolumin systemowy, zgodnie z wybranym trybem startowym (MBR w przypadku systemu BIOS, GPT w przypadku systemu UEFI).
- Dostosuje ustawienia systemu operacyjnego Windows tak, aby mógł on zostać uruchomiony przy użyciu wybranego trybu startowego.

Ustawienie wstępne: **Tak jak na komputerze docelowym.**

Możesz wybrać jedną z poniższych opcji:

© Acronis International GmbH, 2003-2024

- **Tak jak na komputerze docelowym**

  Agent działający na komputerze docelowym wykrywa tryb startowy aktualnie używany przez system Windows i wprowadza stosowne zmiany.

  Jest to najbezpieczniejsza wartość, która automatycznie zapewnia możliwość uruchomienia systemu, chyba że mają zastosowanie poniższe ograniczenia. Ponieważ opcja **Tryb startowy** nie jest dostępna w ramach nośnika startowego, agent na nośniku zawsze działa tak, jakby ta wartość była wybrana.
- **Tak jak na komputerze uwzględnionym w kopii zapasowej**

  Agent działający na komputerze docelowym odczytuje tryb startowy z kopii zapasowej i wprowadza stosowne zmiany. Ułatwia to odzyskanie systemu na innym komputerze, nawet jeśli ten komputer korzysta z innego trybu startowego, a następnie zamianę dysku w komputerze uwzględnionym w kopii zapasowej.
- **BIOS**

  Agent działający na komputerze docelowym odczytuje wprowadza stosowne zmiany, aby umożliwić użycie systemu BIOS.
- **UEFI**

  Agent działający na komputerze docelowym odczytuje wprowadza stosowne zmiany, aby umożliwić użycie systemu UEFI.

W przypadku zmiany tego ustawienia procedura mapowania dysków zostanie ponowiona. Może to potrwać jakiś czas.

Zalecenia

Jeśli trzeba przenieść system Windows między systemami UEFI i BIOS:

- Odzyskaj cały dysk, na którym znajduje się wolumin systemowy. Jeśli odzyskasz tylko wolumin systemowy na istniejącym woluminie, agent nie będzie w stanie prawidłowo zainicjować dysku docelowego.
- Pamiętaj, że system BIOS nie pozwala na stosowanie dysków o pojemności przekraczającej 2 TB.

Ograniczenia

- Przeniesienie między systemami UEFI i BIOS jest obsługiwane w następujących przypadkach:
  - 64-bitowe wersje systemów operacyjnych Windows, począwszy od systemu Windows 7
  - 64-bitowe wersje systemów operacyjnych Windows Server, począwszy od systemu Windows Server 2008 SP1
- Jeśli kopia zapasowa jest przechowywana na urządzeniu taśmowym, przeniesienie między systemami UEFI i BIOS nie jest obsługiwane.

Jeśli przeniesienie między systemami UEFI i BIOS nie jest obsługiwane, agent zachowuje się tak, jakby było wybrane ustawienie **Tak jak na komputerze uwzględnionym w kopii zapasowej**. Jeśli komputer docelowy obsługuje zarówno system UEFI, jak i BIOS, należy ręcznie włączyć tryb startowy odpowiadający pierwotnemu komputerowi. W przeciwnym razie system nie uruchomi się.

© Acronis International GmbH, 2003-2024

Data i godzina plików

Ta opcja jest dostępna tylko podczas odzyskiwania plików.

Opcja określa, czy data i godzina plików mają być odzyskiwane z kopii zapasowej, czy też do plików ma być przypisywana bieżąca data i godzina.

W przypadku włączenia tej opcji plikom będą przypisywane bieżąca data i godzina.

Ustawienie wstępne: **Włączono**.

Obsługa błędów

Umożliwiają one określenie sposobu obsługi błędów, które mogą wystąpić podczas odzyskiwania.

W razie błędu spróbuj ponownie

Ustawienie wstępne: **Włączono. Liczba prób: 30. Odstęp między próbami: 30 s.**

Po wystąpieniu błędu, który można naprawić, program próbuje ponownie wykonać operację zakończoną niepowodzeniem. Można ustawić odstęp między kolejnymi próbami oraz ich liczbę. Ponowne próby zostaną wstrzymane po pomyślnym wykonaniu operacji LUB wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb cichy)

Ustawienie wstępne: **Wyłączono**.

Po włączeniu trybu dyskretnego program automatycznie obsługuje sytuacje wymagające działania użytkownika, jeśli jest to możliwe. Jeśli operacja nie może być kontynuowana bez działania użytkownika, zakończy się niepowodzeniem. Szczegółowe informacje na temat operacji, w tym błędy, które wystąpiły, można znaleźć w dzienniku operacji.

Zapisz informacje o systemie w razie niepowodzenia odzyskiwania z ponownym rozruchem

Ta opcja jest dostępna w przypadku odzyskiwania dysku lub woluminu na komputer fizyczny z systemem Windows lub Linux.

Ustawienie wstępne: **Wyłączono**.

Jeśli ta opcja jest włączona, można wskazać folder na dysku lokalnym (w tym w pamięci flash lub na dysku HDD podłączonym do komputera docelowego) lub w udziale sieciowym, w którym będą zapisywane dziennik, informacje o systemie i pliki zrzutów awaryjnych. Plik ten pomoże pracownikom pomocy technicznej w ustaleniu natury problemu.

Wykluczenia plików

Ta opcja jest dostępna tylko podczas odzyskiwania plików.

© Acronis International GmbH, 2003-2024

Opcja określa, które pliki i foldery należy pominąć w procesie odzyskiwania, a tym samym wykluczyć z listy odzyskiwanych elementów.

Uwaga
Wykluczenia mają wyższy priorytet niż wybór elementów danych do odzyskania. Jeśli na przykład wybierzesz do odzyskania plik MójPlik.tmp i wykluczysz wszystkie pliki .tmp, plik MójPlik.tmp nie zostanie odzyskany.

Zabezpieczenia na poziomie plików

Ta opcja jest dostępna podczas odzyskiwania plików z kopii zapasowych woluminów sformatowanych w systemie plików NTFS wykonanych na poziomie dysku i na poziomie plików.

Opcja określa, czy razem z plikami mają być odzyskiwane uprawnienia do plików pochodzące z systemu NTFS.

Ustawienie wstępne: **Włączono**.

Można wybrać opcję odzyskania uprawnień lub dziedziczenia przez pliki uprawnień NTFS z folderu, do którego są odzyskiwane.

Flashback

Ta opcja jest dostępna w przypadku odzyskiwania dysków i woluminów na komputerach fizycznych oraz maszynach wirtualnych, z wyjątkiem komputerów Mac.

Ta opcja działa tylko wtedy, gdy układ woluminu odzyskiwanego dysku jest dokładnie taki sam jak w przypadku dysku docelowego.

Jeśli ta opcja jest włączona, odzyskiwane są tylko różnice między danymi z kopii zapasowej a danymi dysku docelowego. Przyspiesza to odzyskiwanie komputerów fizycznych i maszyn wirtualnych. Dane są porównywane na poziomie bloków.

W przypadku odzyskiwania komputera fizycznego ustawienie wstępne jest następujące: **Wyłączono**.

W przypadku odzyskiwania maszyny wirtualnej ustawienie wstępne jest następujące: **Włączono**.

Odzyskiwanie pełnej ścieżki

Ta opcja jest dostępna tylko w przypadku odzyskiwania danych z kopii zapasowej na poziomie plików.

Jeśli ta opcja jest włączona, w lokalizacji docelowej zostanie odtworzona pełna ścieżka pliku.

Ustawienie wstępne: **Wyłączono**.

Punkty zamontowania

Ta opcja jest dostępna tylko w systemie Windows w przypadku odzyskiwania danych z kopii zapasowej na poziomie pliku.

© Acronis International GmbH, 2003-2024

Włącz tę opcję, aby odzyskać pliki i foldery przechowywane na zamontowanych woluminach, których kopie zapasowe zostały wykonane przy włączonej opcji Punkty zamontowania.

Ustawienie wstępne: **Wyłączono**.

Ta opcja jest dostępna tylko wtedy, gdy wybrany folder do odzyskania znajduje się wyżej w hierarchii folderów niż punkt zamontowania. Jeśli wskażesz do operacji odzyskiwania foldery znajdujące się wewnątrz punktu zamontowania lub sam punkt zamontowania, wybrane elementy zostaną odzyskane bez względu na wartość opcji **Punkty zamontowania**.

Uwaga
Należy pamiętać, że jeśli wolumin nie jest zamontowany w momencie odzyskiwania, dane zostaną odzyskane bezpośrednio do folderu, który był określony jak punkt zamontowania podczas tworzenia kopii zapasowej.

Wydajność

Ta opcja umożliwia określenie priorytetu procesu odzyskiwania w systemie operacyjnym.

Dostępne są następujące ustawienia: **Niski**, **Normalny**, **Wysoki**.

Ustawienie wstępne: **Normalny**.

Priorytet procesu działającego w systemie określa ilość mocy obliczeniowej procesora i zasobów systemowych przydzielonych do tego procesu. Obniżenie priorytetu odzyskiwania zwolni więcej zasobów na potrzeby pozostałych aplikacji. Podwyższenie priorytetu odzyskiwania może przyspieszyć proces odzyskiwania przez żądanie przydzielenia przez system operacyjny większej ilości zasobów aplikacji odzyskującej. Jednak efekt takiej operacji będzie zależał od całkowitego wykorzystania mocy obliczeniowej procesora oraz innych czynników, takich jak szybkość operacji we/wy na dysku czy natężenie ruchu w sieci.

Polecenia poprzedzające/następujące

Ta opcja umożliwia określenie poleceń wykonywanych automatycznie przed odzyskiwaniem danych i po jego zakończeniu.

Przykład zastosowania poleceń poprzedzających/następujących:

- Uruchomienie polecenia **Checkdisk** w celu znalezienia i naprawienia problemów z logicznym systemem plików, błędów fizycznych lub uszkodzonych sektorów przed rozpoczęciem odzyskiwania lub po jego zakończeniu.

Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause”).

Polecenia po zakończeniu odzyskiwania nie zostaną wykonane, jeśli proces odzyskiwania uruchomi ponownie komputer.

Polecenie poprzedzające odzyskiwanie

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu odzyskiwania

© Acronis International GmbH, 2003-2024

1. Włącz przełącznik **Wykonaj polecenie przed odzyskaniem**.
2. W polu **Polecenie** wpisz polecenie lub wybierz plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause").
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby podaj argumenty wykonania polecenia.
5. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
6. Kliknij **Gotowe**.

Pole wyboru	**Wybór**			
Jeśli wykonanie polecenia się nie powiedzie, zakończ zadanie odzyskiwania niepowodzeniem*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie przeprowadzaj odzyskiwania przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Przeprowadź odzyskiwanie dopiero po pomyślnym wykonaniu polecenia. Zakończ odzyskiwanie niepowodzeniem, jeśli wykonanie polecenia się nie powiodło.	Przeprowadź odzyskiwanie po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N.d.	Przeprowadź odzyskiwanie równolegle z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

* Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera.

Polecenie po zakończeniu odzyskiwania

Aby określić polecenie/plik wykonywalny, które mają zostać wykonane po zakończeniu odzyskiwania

1. Włącz przełącznik **Wykonaj polecenie po odzyskaniu**.
2. W polu **Polecenie** wpisz polecenie lub wybierz plik wsadowy.

© Acronis International GmbH, 2003-2024

3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
5. Jeśli pomyślne wykonanie polecenia ma znaczenie krytyczne, zaznacz pole wyboru **Zakończ odzyskiwanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie**. Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera. W takim przypadku zostanie ustawiony status odzyskiwania **Błąd**.

   Jeśli to pole wyboru nie jest zaznaczone, wynik wykonania polecenia nie wpływa na powodzenie lub niepowodzenie operacji odzyskiwania. Wynik wykonania polecenia można sprawdzić na karcie **Działania**.
6. Kliknij **Gotowe**.

Uwaga
Polecenia po zakończeniu odzyskiwania nie zostaną wykonane, jeśli proces odzyskiwania uruchomi ponownie komputer.

Zmiana identyfikatorów SID

Ta opcja jest dostępna w przypadku odzyskiwania systemu Windows 8.1/Windows Server 2012 R2 lub starszego.

Ta opcja nie działa w przypadku odzyskiwania na maszynę wirtualną przy użyciu agenta dla VMware, agenta dla Hyper-V, agenta dla Scale Computing HC3 lub agenta dla oVirt.

Ustawienie wstępne: **Wyłączono**.

Oprogramowanie może wygenerować unikatowy identyfikator zabezpieczeń (SID komputera) dla odzyskiwanego systemu operacyjnego. Ta opcja jest potrzebna tylko do zapewnienia działania oprogramowania innych firm, które korzysta z identyfikatora SID komputera.

Oficjalnie firma Microsoft nie zapewnia obsługi zmiany identyfikatora SID we wdrażanym lub odzyskiwanym systemie. Dlatego tej opcji używa się na własne ryzyko.

Zarządzanie zasilaniem maszyn wirtualnych

Te opcje są dostępne w przypadku odzyskiwania na maszynę wirtualną przy użyciu agenta dla VMware, agenta dla Hyper-V, agenta dla Virtuozzo, agenta dla Scale Computing HC3 lub agenta dla oVirt.

Przed uruchomieniem odzyskiwania wyłącz docelowe maszyny wirtualne

Ustawienie wstępne: **Włączono**.

Odzyskanie na istniejącą maszynę wirtualną nie jest możliwe, jeśli jest ona w trybie online, dlatego natychmiast po rozpoczęciu odzyskiwania maszyna jest automatycznie wyłączana. Użytkownicy są odłączani od maszyny, a wszelkie niezapisane dane zostaną utracone.

© Acronis International GmbH, 2003-2024

Jeśli wolisz ręcznie wyłączać maszyny wirtualne przed rozpoczęciem odzyskiwania, wyczyść pole wyboru tej opcji.

Włącz docelową maszynę wirtualną po zakończeniu odzyskiwania

Ustawienie wstępne: **Wyłączono**.

Po odzyskaniu maszyny z kopii zapasowej na inną maszynę, w sieci może się pojawić replika istniejącej maszyny. Na wszelki wypadek po zastosowaniu niezbędnych środków ostrożności ręcznie włącz odzyskaną maszynę wirtualną.

Dziennik zdarzeń systemu Windows

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Ta opcja umożliwia określenie, czy agenty muszą rejestrować zdarzenia operacji odzyskiwania w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, uruchom plik eventvwr.exe lub wybierz **Panel sterowania** > **Narzędzia administracyjne** > **Podgląd zdarzeń**). Zdarzenia, które mają być rejestrowane, można filtrować.

Ustawienie wstępne: **Wyłączono**.

Operacje dotyczące kopii zapasowych

Karta Magazyn kopii zapasowych

Karta **Magazyn kopii zapasowych** zapewnia dostęp do wszystkich kopii zapasowych, w tym kopii komputerów w trybie offline, kopii komputerów, które nie są już zarejestrowane w usłudze Cyber Protection, kopii w chmurach publicznych, takich jak Microsoft Azure, oraz osieroconych kopii zapasowych[1].

Kopie zapasowe utworzone za pomocą narzędzia `acrocmd` są oznaczane jako osierocone. Kopie zapasowe utworzone w wersji 12.5 produktu również są identyfikowane jako osierocone.

Uwaga
Uwaga: za osierocone kopie zapasowe również są naliczane opłaty.

Kopie zapasowe przechowywane w lokalizacji współużytkowanej (takiej jak udział SMB lub NFS) są widoczne dla wszystkich użytkowników mających uprawnienia do odczytu w danej lokalizacji.

W systemie Windows pliki kopii zapasowych dziedziczą uprawnienia dostępu z folderu nadrzędnego. Dlatego zalecamy ograniczenie uprawnień do odczytu w przypadku tego folderu.

W chmurze użytkownicy mają dostęp tylko do własnych kopii zapasowych.

Administrator może przeglądać kopie zapasowe tworzone w chmurze w ramach każdego konta należącego do określonej jednostki lub firmy i jej grup podrzędnych, zaznaczając chmurę powiązaną

[1]Osierocona kopia zapasowa to kopia zapasowa, która nie jest już powiązana z żadnym planem ochrony.

© Acronis International GmbH, 2003-2024

z tym kontem. Aby wybrać urządzenie, które ma być używane do uzyskiwania danych z chmury, kliknij **Zmień** w wierszu **Komputer używany do przeglądania**. Na karcie **Magazyn kopii zapasowych** są wyświetlane kopie zapasowe wszystkich komputerów kiedykolwiek zarejestrowanych w ramach wybranego konta.

Kopie zapasowe utworzone przez *dostępnego w chmurze* agenta dla usługi Microsoft 365 oraz kopie zapasowe Google Workspacesą wyświetlane nie w lokalizacji **Chmura**, tylko w osobnej sekcji o nazwie **Kopie zapasowe aplikacji w chmurze**.

Lokalizacje kopii zapasowych używane w planach ochrony są automatycznie dodawane na karcie **Magazyn kopii zapasowych**. Aby dodać folder niestandardowy (na przykład odłączane urządzenie USB) do listy lokalizacji kopii zapasowych, kliknij **Przeglądaj** i określ ścieżkę folderu.

Jeśli niektóre kopie zapasowe zostały dodane lub usunięte za pomocą menedżera plików, kliknij ikonę koła zębatego obok nazwy lokalizacji, a następnie kliknij **Odśwież**.

Ostrzeżenie!
Nie próbuj edytować plików kopii zapasowych ręcznie, ponieważ może to poskutkować uszkodzeniem plików i bezużytecznością tych kopii zapasowych. Ponadto zalecamy korzystanie z replikacji kopii zapasowych, a nie ręczne przenoszenie plików kopii zapasowych.

Jeśli z usługi zostaną usunięte wszystkie komputery, które kiedykolwiek miały tworzone kopie zapasowe w danej lokalizacji kopii zapasowych, to lokalizacja ta (z wyjątkiem chmury) zniknie z karty **Magazyn kopii zapasowych**. Eliminuje to konieczność płacenia za kopie zapasowe przechowywane w tej lokalizacji. Gdy tylko znów zostanie w niej utworzona jakaś kopia zapasowa, lokalizacja zostanie ponownie dodana wraz ze wszystkimi przechowywanymi w niej kopiami zapasowymi.

Na karcie **Magazyn kopii zapasowych** można filtrować kopie zapasowe z listy przy użyciu następujących kryteriów:

- **Tylko z danymi do analizy śledczej** — zostaną wyświetlone tylko kopie zapasowe zawierające dane przeznaczone do analizy śledczej.
- **Tylko kopie zapasowe przed aktualizacją utworzone przez funkcję Zarządzanie poprawkami** — zostaną wyświetlone tylko kopie zapasowe utworzone w ramach zarządzania poprawkami przed instalacją poprawek.

Aby wybrać punkt odzyskiwania na karcie Magazyn kopii zapasowych

1. Na karcie **Magazyn kopii zapasowych** wybierz lokalizację, w której są przechowywane kopie zapasowe.

   W oprogramowaniu zostaną wyświetlone wszystkie kopie zapasowe z wybranej lokalizacji, które można zobaczyć z danego konta. Kopie te są zestawione w grupy. Nazwy grup są oparte na następującym szablonie:

   `<nazwa komputera> – <nazwa planu ochrony>`
2. Wybierz grupę, z której chcesz odzyskać dane.
3. [Opcjonalnie] Kliknij **Zmień** obok pozycji **Komputer używany do przeglądania**, a następnie wybierz inny komputer. Niektóre kopie zapasowe można przeglądać tylko przy użyciu

© Acronis International GmbH, 2003-2024

określonych agentów. Na przykład w celu przeglądania kopii zapasowych baz danych programu Microsoft SQL Server trzeba wybrać komputer z agentem dla SQL.

Ważne
Warto pamiętać, że **Komputer używany do przeglądania** jest domyślnym miejscem docelowym odzyskiwania z kopii zapasowej komputera fizycznego. Po wybraniu punktu odzyskiwania i kliknięciu **Odzyskaj** dokładnie sprawdź ustawienie **Komputer docelowy**, aby się upewnić, że został wybrany komputer, na który chcesz odzyskać dane. Aby zmienić miejsce docelowe odzyskiwania, określ w polu **Komputer używany do przeglądania** inny komputer.

4. Kliknij **Pokaż kopie zapasowe**.
5. Wybierz punkt odzyskiwania.

Aby dodać lokalizację kopii zapasowej

Uwaga
Ta operacja jest dostępna tylko w przypadku dysponowania agentem online.

Na karcie **Magazyn kopii zapasowych** kliknij **Dodaj lokalizację**.

Wybierz lokalizację spośród następujących typów lokalizacji, a następnie kliknij **Gotowe**:

- Folder lokalny
- Folder sieciowy
- Secure Zone
- Folder NFS
- Chmura publiczna

Montowanie woluminów z kopii zapasowej

Montowanie woluminów z kopii zapasowej na poziomie dysku pozwala na dostęp do woluminów w taki sam sposób jak do dysków fizycznych.

Zamontowanie woluminów w trybie do odczytu i zapisu umożliwia modyfikowanie zawartości kopii zapasowej, czyli zapisywanie, przenoszenie, tworzenie, usuwanie plików lub folderów i uruchamianie programów składających się z jednego pliku. W tym trybie oprogramowanie tworzy przyrostową kopię zapasową zawierającą zmiany wprowadzone w zawartości kopii zapasowej. Uwaga: żadna z późniejszych kopii zapasowych nie będzie zawierać tych zmian.

Wymagania

- Ta funkcja jest dostępna tylko w przypadku korzystania z Eksploratora plików w systemie Windows.
- Na komputerze wykonującym operację montowania musi być zainstalowany agent dla systemu Windows.

© Acronis International GmbH, 2003-2024

- Wersja systemu Windows działającego na komputerze musi obsługiwać system plików z kopii zapasowej.
- Kopia zapasowa musi być przechowywana w folderze lokalnym, udziale sieciowym (SMB/CIFS) lub strefie Secure Zone.

Scenariusze użycia

- Udostępnianie danych

  Zamontowane woluminy można łatwo udostępniać przez sieć.
- Rozwiązanie odzyskiwania z wykorzystaniem rezerwowej bazy danych

  Zamontuj wolumin zawierający bazę danych SQL z komputera, który ostatnio uległ awarii. Umożliwi to dostęp do bazy danych do czasu odzyskania uszkodzonego komputera. Metody tej można też używać do odzyskiwania granularnego danych programu Microsoft SharePoint przy użyciu programu SharePoint Explorer.
- Usuwanie wirusów w trybie offline

  Jeśli komputer jest zainfekowany, zamontuj jego kopię zapasową, oczyść ją za pomocą programu antywirusowego (lub znajdź ostatnią niezainfekowaną kopię zapasową), a następnie odzyskaj komputer z tej kopii.
- Sprawdzanie pod kątem błędów

  Jeśli odzyskanie ze zmianą rozmiaru woluminu się nie powiodło, przyczyną może być błąd w systemie plików w kopii zapasowej. Zamontuj kopię zapasową w trybie do odczytu i zapisu. Następnie sprawdź, czy w zamontowanym woluminie nie ma błędów, korzystając z polecenia `chkdsk /r`. Po naprawieniu błędów i utworzeniu nowej przyrostowej kopii zapasowej odzyskaj system z tej kopii.

Aby zamontować wolumin z kopii zapasowej

1. W Eksploratorze plików przejdź do lokalizacji kopii zapasowej.
2. Kliknij dwukrotnie plik kopii zapasowej. Nazwy plików mają następującą strukturę:

   `<nazwa komputera> – <GUID planu ochrony>`
3. Jeśli kopia zapasowa jest zaszyfrowana, wprowadź hasło szyfrowania. W przeciwnym razie pomiń ten krok.

   W Eksploratorze plików zostaną wyświetlone punkty odzyskiwania.
4. Kliknij dwukrotnie odpowiedni punkt odzyskiwania.

   W Eksploratorze plików zostaną wyświetlone woluminy z kopii zapasowej.

   Uwaga
   Kliknij dwukrotnie wolumin, aby przejrzeć jego zawartość. Pliki i foldery z kopii zapasowej możesz skopiować do dowolnego folderu w systemie plików.
5. Kliknij prawym przyciskiem myszy montowany wolumin, a następnie wybierz jedną z następujących opcji:

© Acronis International GmbH, 2003-2024

a. **Zamontuj**

Uwaga
W trybie do odczytu/zapisu można zamontować tylko ostatnią kopię zapasową z archiwum (ciągu kopii zapasowych).

b. **Zamontuj w trybie tylko do odczytu**.

6. Jeśli kopia zapasowa jest przechowywana w udziale sieciowym, podaj poświadczenia dostępu. W przeciwnym razie pomiń ten krok.

   Oprogramowanie zamontuje wybrany wolumin. Do tego woluminu zostanie przypisana pierwsza wolna litera.

Aby odmontować wolumin

1. W Eksploratorze plików przejdź do obszaru **Komputer** (**Ten komputer PC** w systemie Windows 8.1 lub nowszym).
2. Kliknij prawym przyciskiem myszy zamontowany wolumin.
3. Kliknij **Odmontuj**.
4. [Opcjonalnie] Jeśli wolumin został zamontowany w trybie do odczytu i zapisu, a jego zawartość została zmodyfikowana, określ, czy ma zostać utworzona przyrostowa kopia zapasowa zawierające te zmiany. W przeciwnym razie pomiń ten krok.

Oprogramowanie odmontuje wybrany wolumin.

Sprawdzanie poprawności kopii zapasowych

Sprawdzanie poprawności kopii zapasowej oznacza sprawdzanie, czy uda się odzyskać z niej dane. Więcej informacji na temat tej operacji można znaleźć w sekcji "Sprawdzanie poprawności" (s. 234).

Uwaga
Ta funkcja jest dostępna w ramach dzierżawców-klientów, dla których włączono limit **Zaawansowane kopie zapasowe — serwery** lub **Zaawansowane kopie zapasowe — NAS** w ramach pakietu Advanced Backup.

Aby sprawdzić poprawność kopii zapasowej

1. Wybierz obciążenie uwzględnione w kopii zapasowej.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli obciążenie jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:

   - Jeśli lokalizacją kopii zapasowych jest chmura lub magazyn współużytkowany (czyli taki, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, a następnie wybierz obciążenie docelowe będące w trybie online i punkt odzyskiwania.

 © Acronis International GmbH, 2003-2024

- Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych. Więcej informacji na temat dostępnych tam kopii zapasowych można znaleźć w sekcji "Karta Magazyn kopii zapasowych" (s. 566).

4. Kliknij ikonę koła zębatego, a następnie kliknij **Sprawdź poprawność**.
5. Wybierz agenta, który ma przeprowadzić sprawdzanie poprawności.
6. Wybierz metodę sprawdzania poprawności.
7. Jeśli kopia zapasowa jest zaszyfrowana, podaj hasło szyfrowania.
8. Kliknij **Rozpocznij**.

Eksportowanie kopii zapasowych

Operacja eksportu polega na utworzeniu we wskazanej lokalizacji samowystarczalnej kopii wybranej kopii zapasowej. Oryginalna kopia zapasowa pozostaje niezmieniona. Eksport kopii zapasowych umożliwia wyodrębnienie określonej kopii zapasowej z ciągu przyrostowych i różnicowych kopii zapasowych w celu szybkiego jej odzyskania, zapisania na nośniku wymiennym bądź odłączanym albo w innym celu.

Uwaga
Ta funkcja jest dostępna w ramach dzierżawców-klientów, dla których włączono limit **Zaawansowane kopie zapasowe — serwery** lub **Zaawansowane kopie zapasowe — NAS** w ramach pakietu Advanced Backup.

Wynikiem operacji eksportu zawsze jest pełna kopia zapasowa. Jeśli zechcesz zreplikować cały ciąg kopii zapasowych do innej lokalizacji i zachować wiele punktów odzyskiwania, użyj planu replikacji kopii zapasowej. Więcej informacji na temat tego planu można znaleźć w sekcji "Replikacja kopii zapasowej" (s. 230).

Nazwa pliku wyeksportowanej kopii zapasowej będzie taka sama jak nazwa pliku oryginalnej kopii zapasowej, z wyjątkiem kolejnego numeru. Jeśli do danej lokalizacji zostanie wyeksportowanych kilka kopii zapasowych z tego samego ciągu kopii zapasowych, do nazw ich plików — z wyjątkiem pierwszego — zostanie dodany czterocyfrowy kolejny numer.

Wyeksportowana kopia zapasowa dziedziczy ustawienia szyfrowania i hasło po oryginalnej kopii zapasowej. W przypadku eksportowania zaszyfrowanej kopii zapasowej trzeba podać hasło.

Aby wyeksportować kopię zapasową

1. Wybierz obciążenie uwzględnione w kopii zapasowej.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji. Jeśli obciążenie jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub magazyn współużytkowany (czyli taki, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, a następnie wybierz obciążenie

© Acronis International GmbH, 2003-2024

docelowe będące w trybie online i punkt odzyskiwania.

- Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych. Więcej informacji na temat dostępnych tam kopii zapasowych można znaleźć w sekcji "Karta Magazyn kopii zapasowych" (s. 566).

4. Kliknij ikonę koła zębatego, a następnie kliknij **Eksportuj**.
5. Wybierz agenta, który ma przeprowadzić eksport.
6. Jeśli kopia zapasowa jest zaszyfrowana, podaj hasło szyfrowania. W przeciwnym razie pomiń ten krok.
7. Określ miejsce docelowe eksportu.
8. Kliknij **Rozpocznij**.

Usuwanie kopii zapasowych

Archiwum kopii zapasowej zawiera co najmniej jedną kopię zapasową. Możesz usunąć określone kopie zapasowe (punkty odzyskiwania) dostępne w archiwum lub całe archiwum.

Usunięcie archiwum kopii zapasowych powoduje usunięcie wszystkich znajdujących się w nim kopii zapasowych. Usunięcie wszystkich kopii zapasowych maszyny powoduje usunięcie archiwów kopii zapasowych zawierających te kopie zapasowe.

Możesz usunąć kopie zapasowe za pomocą konsoli Cyber Protect — na karcie **Urządzenia** oraz karcie **Magazyn kopii zapasowych**. Możesz też usunąć kopie zapasowe z chmury za pomocą konsoli Web Restore.

Ostrzeżenie!
Jeśli niezmienny magazyn jest wyłączony, dane kopii zapasowej są trwale usuwane i nie można ich odzyskać.

Aby usunąć kopie zapasowe lub archiwa kopii zapasowych

Na karcie Urządzenia

Ta procedura dotyczy tylko maszyn online.

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz kopie zapasowe maszyn, które chcesz usunąć.
3. Kliknij **Odzyskiwanie**.
4. [Jeśli jest dostępna więcej niż jedna lokalizacja kopii zapasowych] Wybierz lokalizację kopii zapasowych.
5. [Aby usunąć wszystkie kopie zapasowe maszyny] Kliknij **Usuń wszystko**.
   Usunięcie wszystkich kopii zapasowych powoduje usunięcie również archiwów kopii zapasowych zawierających te kopie zapasowe.
6. [Aby usunąć określoną kopię zapasową] Wybierz kopię zapasową (punkt odzyskiwania), którą chcesz usunąć, a następnie kliknij **Czynności** > **Usuń**.

© Acronis International GmbH, 2003-2024

7. [W przypadku usuwania wszystkich kopii zapasowych] Zaznacz pole wyboru, a następnie kliknij **Usuń**, aby potwierdzić decyzję.
8. [W przypadku usuwania określonej kopii zapasowej] Kliknij **Usuń**, aby potwierdzić decyzję.

Na karcie Magazyn kopii zapasowych

Ta procedura dotyczy maszyn w trybie online i offline.

1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych**.
2. Wybierz lokalizację, z której chcesz usunąć kopie zapasowe.
3. Wybierz archiwum kopii zapasowych, z którego chcesz usunąć kopie zapasowe.
   Nazwa archiwum jest zdefiniowana według następującego szablonu:
   - Archiwa kopii zapasowych innych niż kopie zapasowe z chmury do chmury: <nazwa maszyny> - <nazwa planu ochrony>
   - Archiwa kopii zapasowych z chmury do chmury: <nazwa użytkownika> lub <nazwa dysku> lub <nazwa zespołu> - <usługa chmurowa> - <nazwa planu ochrony>
4. [Aby usunąć całe archiwum kopii zapasowych] Kliknij **Usuń**.
   Usunięcie archiwum kopii zapasowych powoduje usunięcie wszystkich kopii zapasowych zawartych w tym archiwum.
5. [Aby usunąć określoną kopię zapasową z archiwum kopii zapasowych] Kliknij **Pokaż kopie zapasowe**.
   a. Wybierz kopię zapasową (punkt odzyskiwania), którą chcesz usunąć.
   b. Kliknij **Czynności** > **Usuń**.
6. [W przypadku usuwania archiwum kopii zapasowych] Zaznacz pole wyboru, a następnie kliknij **Usuń**, aby potwierdzić decyzję.
7. [W przypadku usuwania określonej kopii zapasowej] Kliknij **Usuń**, aby potwierdzić decyzję.

W konsoli Web Restore

Ta procedura dotyczy tylko archiwów kopii zapasowych w chmurze.

1. W konsoli Cyber Protection przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz kopie zapasowe maszyn, które chcesz usunąć, a następnie kliknij **Odzyskiwanie**.
3. [Jeśli są dostępne różne lokalizacje kopii zapasowych] Wybierz lokalizację kopii zapasowych, a następnie kliknij **Więcej metod odzyskiwania**.
4. Kliknij **Pobierz pliki**.
   Nastąpi przekierowanie do konsoli Web Restore.
5. W konsoli Web Restore w obszarze **Komputery** kliknij nazwę maszyny.
6. W obszarze **Ostatnia wersja** kliknij datę, a następnie kliknij **Usuń**.
   Czynność ta jest dostępna wyłącznie na poziomie archiwum kopii zapasowych. Nie można wyświetlać bardziej szczegółowych elementów archiwum ani usuwać z niego określonych kopii zapasowych.
7. Kliknij **Usuń**, aby potwierdzić decyzję.

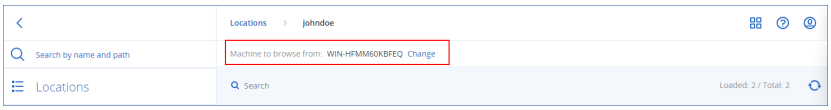
© Acronis International GmbH, 2003-2024

Usuwanie kopii zapasowych poza konsolą Cyber Protect

Zalecamy usuwanie kopii zapasowych za pomocą konsoli Cyber Protect. W przypadku usunięcia kopii zapasowych z chmury za pomocą konsoli Web Restore lub usunięcia lokalnych kopii zapasowych za pomocą menedżera plików trzeba odświeżyć lokalizację kopii zapasowych, aby zsynchronizować zmiany z konsolą Cyber Protect.

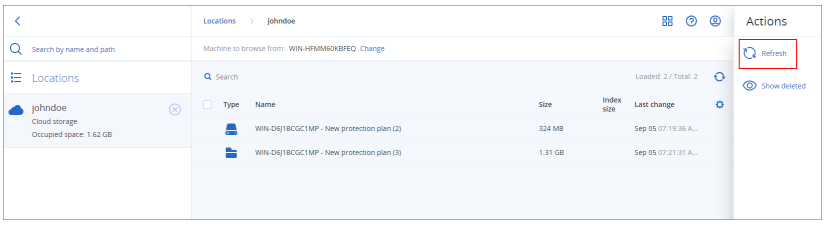
Wymaganie wstępne

- Agent online, który może uzyskać dostęp do danej lokalizacji kopii zapasowych, musi być wybrany jako **Komputer używany do przeglądania** w konsoli Cyber Protect.



Aby odświeżyć lokalizację kopii zapasowych

1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych**.
2. Wybierz lokalizację kopii zapasowych, w której zapisano usunięte kopie zapasowe.
3. W panelu **Czynności** kliknij **Odśwież**.



Opis wykrywania wąskich gardeł

Funkcja wykrywania wąskich gardeł ułatwia ustalanie, w jakich obszarach można poprawić wydajność — wskazuje ona, który komponent systemu był najwolniejszy podczas procesu tworzenia kopii zapasowej lub odzyskiwania.

Wąskie gardła występują *zawsze*, w każdym zdarzeniu transmisji, więc nie oznaczają, że trzeba je wyeliminować. Operacje tworzenia kopii zapasowych mogą być wystarczająco szybkie i doskonale spełniać wymogi dotyczące okien na utworzenie kopii zapasowej, a także umów SLA, więc wąskich gardeł zwykle nie trzeba eliminować.

Wąskie gardła można łatwo przeglądać i monitorować na karcie **Szczegóły działania**. W tym celu w konsoli Cyber Protect przejdź do sekcji **Monitorowanie > Działania** i kliknij odpowiednie działanie. Dodatkowe informacje na temat wyświetlania wąskich gardeł można znaleźć w sekcjach "Wyświetlanie szczegółów wąskich gardeł" (s. 576) i "W przypadku jakich obciążeń, agentów i lokalizacji kopii można wyświetlać wąskie gardła?" (s. 578).

© Acronis International GmbH, 2003-2024

Co to jest wąskie gardło?

Wąskie gardła są zwykle powodowane przez powolny komponent w łańcuchu przetwarzania — innymi słowy, komponent, na który czekają inne komponenty.

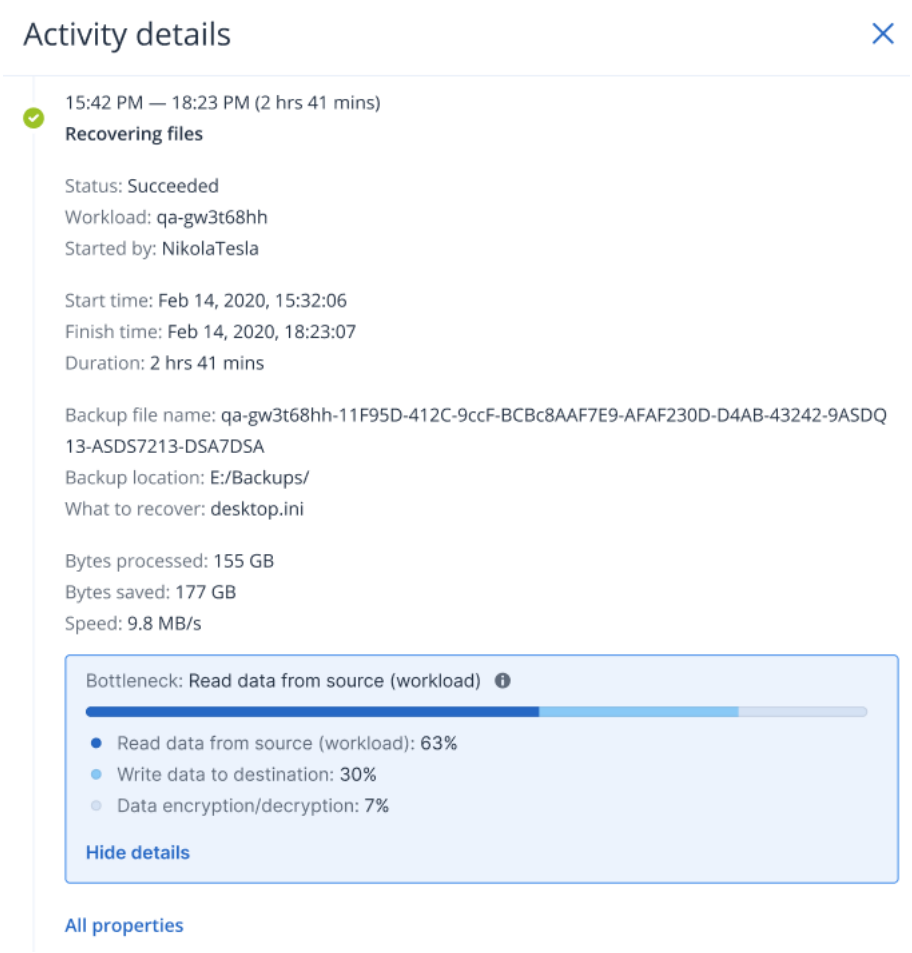
Funkcja wykrywania wąskich gardeł umożliwia monitorowanie tych powolnych komponentów podczas procesu tworzenia kopii zapasowych i odzyskiwania, a tym samym pomaga w ustaleniu, który z poniższych typów komponentów jest najwolniejszy:

- **Źródło**: na pierwszy rzut oka można określić, czy szybkość odczytu ze źródła kopii zapasowej / odzyskiwania powoduje powstanie wąskiego gardła.
- **Miejsce docelowe**: można sprawdzić, czy szybkość zapisu w miejscu docelowym kopii zapasowej / odzyskiwania ma negatywny wpływ na wydajność.
- **Agent**: można sprawdzić, czy agent wystarczająco szybko przetwarza dane.

Typ wąskiego gardła, niezależnie od tego, czy jest ono powodowane przez źródło, miejsce docelowe czy agenta, może być różny na różnym etapie procesu tworzenia kopii zapasowych / odzyskiwania. Wartości procentowe widoczne w sekcji **Wąskie gardło** na karcie **Szczegóły działania** (na przykład **Odczyt danych ze źródła (obciążenia): 63%**) reprezentują procent czasu, w którym występowało wąskie gardło danego typu. W tym przypadku przez 63% czasu odzyskiwania wąskim gardłem był odczyt danych, innymi słowy, mała szybkość odczytu danych z archiwum kopii zapasowych przez agenta.

Przez 30% czasu z kolei wąskie gardło było spowodowane niską szybkością zapisu danych w miejscu docelowym odzyskiwania (**Zapis danych w miejscu docelowym: 30%**).

© Acronis International GmbH, 2003-2024



Uwaga
Normalnym zachowaniem jest wyświetlanie statystyk wąskich gardeł na karcie **Szczegóły działania**. Statystyki te są dostępne tylko w przypadku zadań trwających dłużej niż minutę.

Jak zredukować wąskie gardła

Jak już wspomniano, funkcja wykrywania wąskich gardeł wyróżnia przepływy danych między komponentami kopii zapasowej związane z *odczytem* i *zapisem*. Statystyki *odczytu* odnoszą się do przepływu danych ze źródła danych do agenta, który wykonuje operację tworzenia kopii zapasowej / odzyskiwania, a statystyki *zapisu* dotyczą przepływu danych między agentem a archiwum kopii zapasowych (miejscem docelowym).

Aby zredukować wąskie gardła i poprawić wydajność przepływu danych podczas odczytu/zapisu, należy przeanalizować kanał między agentem a źródłem danych / archiwum kopii zapasowych. Na przykład można spróbować przeprowadzić analizę porównawczą dysków twardych, jeśli agent tworzy kopie zapasowe jakichś plików lokalnych.

Wyświetlanie szczegółów wąskich gardeł

Możesz wyświetlić wykryte wąskie gardła dotyczące operacji tworzenia dowolnego typu kopii zapasowych, replikacji kopii zapasowych lub procesu odzyskiwania (do dowolnego typu folderu

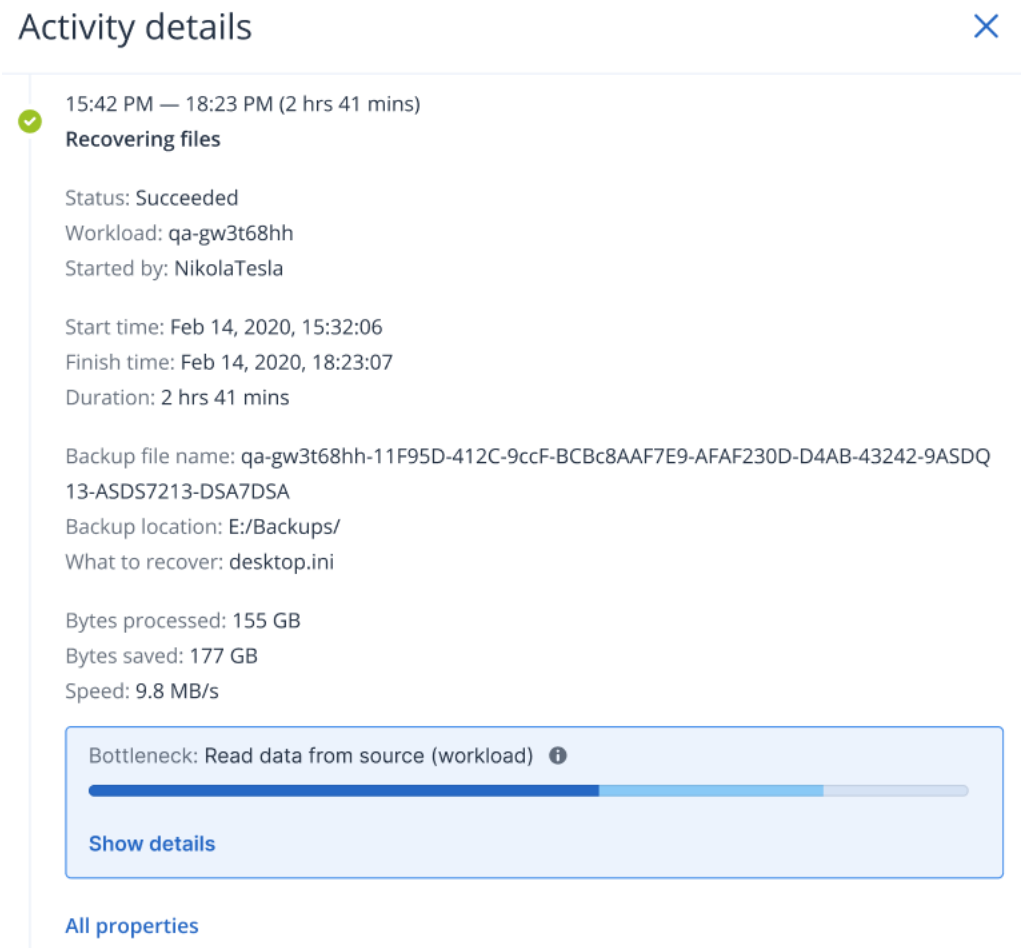
© Acronis International GmbH, 2003-2024

docelowego lub lokalizacji docelowej), w tym kopii zapasowych maszyn wirtualnych, kopii zapasowych komputerów i kopii zapasowych plików/folderów. Możesz też wyświetlić wąskie gardła dotyczące replikacji maszyn wirtualnych i działań związanych z powrotem po awarii.

Dodatkowe informacje na temat definicji i podstawowych pojęć dotyczących typów wąskich gardeł można znaleźć w sekcji "Opis wykrywania wąskich gardeł" (s. 574).

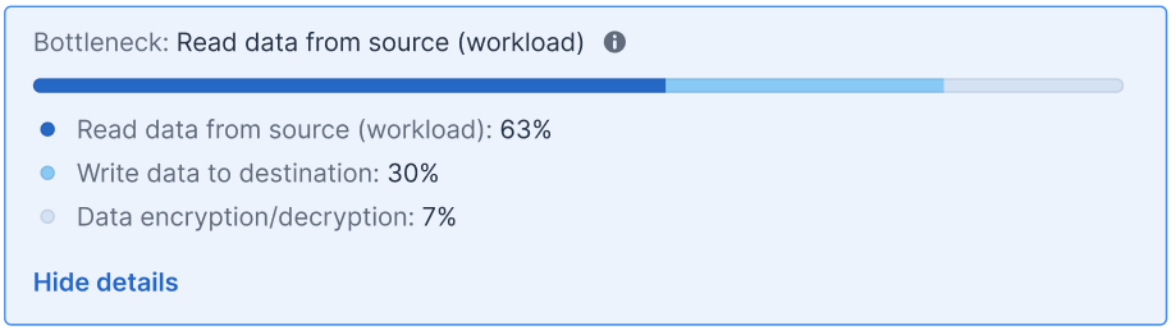
Aby wyświetlić szczegóły wąskich gardeł

1. W konsoli Cyber Protect przejdź do sekcji **Monitorowanie > Działania**.
2. Kliknij odpowiednie działanie.
   Na karcie **Szczegóły działania** sekcja **Wąskie gardło** jest oznaczona kolorem niebieskim.



3. Kliknij **Pokaż szczegóły**, aby wyświetlić najczęściej występujące wąskie gardło podczas operacji tworzenia kopii zapasowych / odzyskiwania.
   Sekcję **Wąskie gardło** można rozwinąć, aby wyświetlić zestawienie typów napotkanych wąskich gardeł.

© Acronis International GmbH, 2003-2024



W powyższym przykładzie wąskie gardło, odpowiedzialne za 63% czasu całego procesu, było spowodowane przez operację *Odczyt* (wykonywaną przez agenta).

Uwaga
Wartości wąskich gardeł są dynamicznie aktualizowane co minutę, gdy jest wykonywane dane działanie.

W przypadku jakich obciążeń, agentów i lokalizacji kopii można wyświetlać wąskie gardła?

Wykrywanie wąskich gardeł jest dostępne w przypadku następujących typów obciążeń, agentów i lokalizacji kopii zapasowych:

- Kopie zapasowe na poziomie dysku/obrazu, które są wykonywane z zastosowaniem następujących narzędzi:
  - Agent dla Azure
  - Agent dla systemu Windows
  - Agent dla systemu Linux
  - Agent dla systemu MAC
  - Agent dla VMware (zarówno urządzenie wirtualne, jak i Windows, w tym takie działania jak replikacja maszyn wirtualnych i powrót po awarii z repliki [przywracanie z repliki])
  - Agent dla Hyper-V
  - Agent dla Scale Computing
  - Agent dla oVirt (KVM)
  - Agent dla Virtuozzo Infrastructure Platform
  - Agent dla Virtuozzo
  - Agent dla VMware Cloud Director (vCD-BA)
- Kopie zapasowe na poziomie plików
  - Agent dla systemu Windows
  - Agent dla systemu Linux
  - Agent dla systemu MAC

© Acronis International GmbH, 2003-2024

- Kopie zapasowe na poziomie aplikacji
  - Agent dla SQL
  - Agent dla programu Exchange
  - Agent dla MySQL/MariaDB
  - Agent dla programu Oracle
  - Agent dla SAP HANA
- Lokalizacje kopii zapasowych
  - Acronis Cloud Storage (w tym magazyny hostowane przez partnerów)
  - Chmura publiczna
  - Udziały sieciowe (SMB + NFS)
  - Foldery lokalne
  - Lokalizacje zdefiniowane za pomocą skryptu
  - Acronis Secure Zone

Tworzenie kopii zapasowych obciążeń w chmurach publicznych

Uwaga
Funkcja ta wchodzi w skład pakietu Zaawansowane tworzenie kopii zapasowych, który z kolei stanowi część usługi Cyber Protection. Uwaga: w przypadku dodania tej funkcji do planu ochrony mogą być naliczane dodatkowe opłaty.

Usługi chmur publicznych, takie jak Microsoft Azure i Amazon S3 (Simple Storage Service), można wybierać jako miejsca docelowe kopii zapasowych w konsoli Cyber Protect.

Aby móc skonfigurować lokalizacje kopii zapasowych w chmurze publicznej, musisz być administratorem firmy lub administratorem jednostki albo mieć jedną z następujących ról zdefiniowanych w usłudze Cyber Protection: Administrator środowiska cybernetycznego, Administrator lub Użytkownik.

Definiowanie lokalizacji kopii zapasowych na platformie Microsoft Azure

Uwaga
Aby móc skonfigurować lokalizacje kopii zapasowych na platformie Microsoft Azure, trzeba mieć zdefiniowaną jedną z następujących ról w usłudze Cyber Protection: Administrator firmy, Użytkownik, Administrator środowiska cybernetycznego.

© Acronis International GmbH, 2003-2024

Aby utworzyć kopię zapasową obciążenia na platformie Microsoft Azure, trzeba zdefiniować lokalizację kopii zapasowych na platformie Microsoft Azure w konsoli Cyber Protect i ustanowić połączenie z odpowiednią subskrypcją platformy Microsoft Azure. Można to zrobić następująco:

- Podczas tworzenia lub edytowania planu ochrony.
- Podczas definiowania lokalizacji magazynów kopii zapasowych i zarządzania nimi.

Ważne
Kopie zapasowe obciążeń na platformie Microsoft Azure mogą tworzyć zarówno administratorzy, jak i użytkownicy niebędący administratorami.

Użytkownicy niebędący administratorami mogą dodać dostęp do subskrypcji platformy Microsoft Azure (zobacz sekcję "Zarządzanie dostępem do subskrypcji platformy Microsoft Azure" (s. 591)), ale plany ochrony mogą stosować tylko wtedy, gdy lokalizacja kopii zapasowych jest połączona z subskrypcją platformy Microsoft Azure, którą sami dodali, oraz w przypadku obciążeń zarejestrowanych w konsoli Cyber Protect przy użyciu ich nazwy użytkownika.

Administratorzy mogą stosować plany ochrony, gdy lokalizacja kopii zapasowych jest połączona z subskrypcjami platformy Microsoft Azure, które zostały dodane przez nich lub przez innego administratora, oraz w przypadku obciążeń zarejestrowanych w konsoli Cyber Protect przy użyciu dowolnej nazwy użytkownika.

Aby zdefiniować lokalizację kopii zapasowych na platformie Microsoft Azure

1. W konsoli Cyber Protect wykonaj jedną z następujących czynności:
   - Jeśli tworzysz lub edytujesz plan ochrony, przejdź do sekcji **Urządzenia** i wybierz obciążenie, którego kopię zapasową chcesz utworzyć na platformie Microsoft Azure. W sekcji **Kopia zapasowa** planu ochrony wybranego obciążenia kliknij łącze w wierszu **Miejsce docelowe kopii zapasowej**.
     Dodatkowe informacje na temat pracy z planami ochrony można znaleźć w sekcji "Plany ochrony i moduły" (s. 221).
   - Jeśli zarządzasz lokalizacjami magazynów kopii zapasowych i chcesz dodać platformę Microsoft Azure jako nową lokalizację, przejdź do sekcji **Magazyn kopii zapasowych**.
     Dodatkowe informacje na temat zarządzania lokalizacjami magazynów kopii zapasowych można znaleźć w sekcji "Karta Magazyn kopii zapasowych" (s. 566).
2. Kliknij **Dodaj lokalizację**.
3. Z listy rozwijanej **Chmury publiczne** wybierz **Microsoft Azure**.
4. Jeśli odpowiednia subskrypcja platformy Microsoft Azure jest już zarejestrowana w konsoli Cyber Protect, wybierz ją na liście subskrypcji.
   Jeśli odpowiednia subskrypcja nie jest zarejestrowana w konsoli Cyber Protect, kliknij **Dodaj** i w wyświetlonym oknie dialogowym kliknij **Zaloguj się**. Nastąpi przekierowanie do strony logowania na koncie Microsoft. Dodatkowe informacje na temat dodawania i definiowania dostępu do

© Acronis International GmbH, 2003-2024

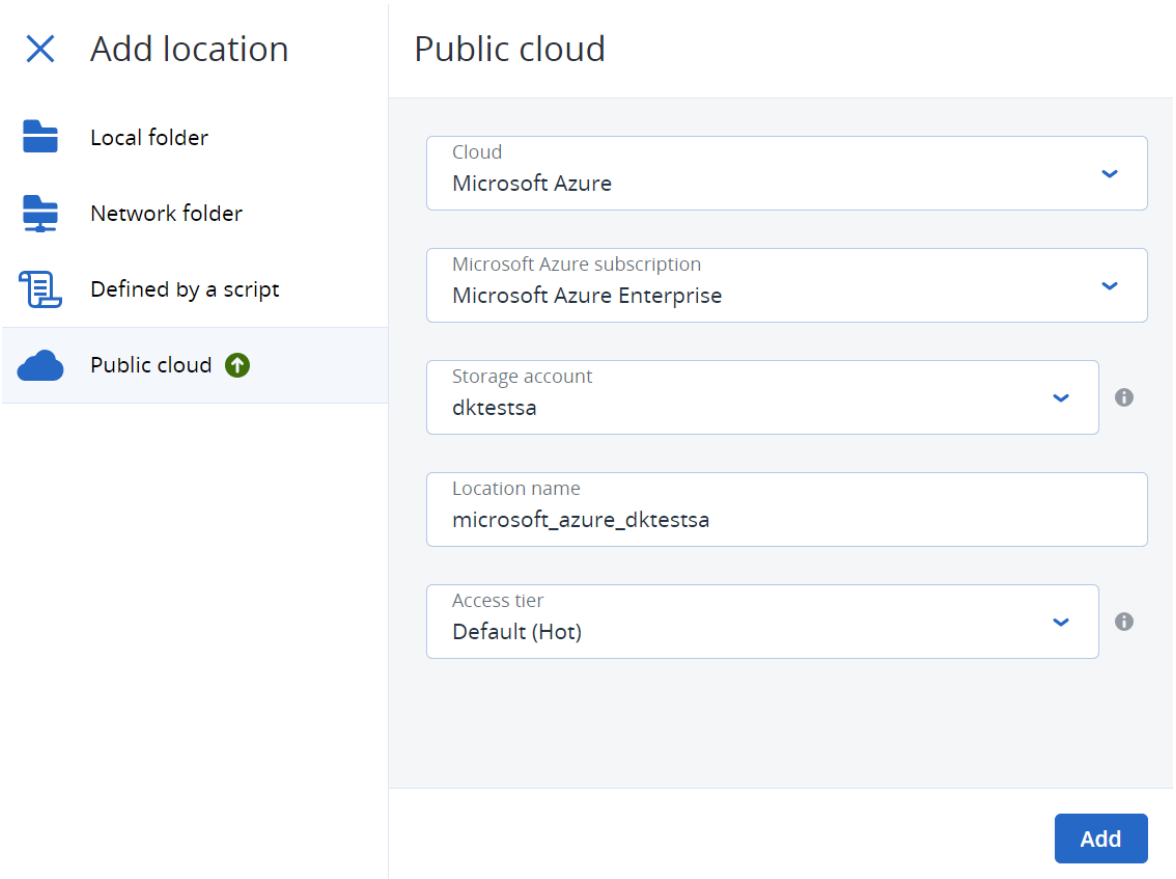
subskrypcji platformy Microsoft Azure można znaleźć w sekcji "Dodawanie dostępu do subskrypcji platformy Microsoft Azure" (s. 592).

5. W polu **Konto magazynu** wybierz odpowiednie konto.

Uwaga
Obecnie są obsługiwane tylko konta magazynów Microsoft Azure ze zwykłymi sufiksami punktów końcowych, które zawierają `core.windows.net`. Ponadto wybrane konto magazynu musi być kontem typu StorageV2.

Pola **Nazwa lokalizacji** i **Poziom dostępu** są domyślnie automatycznie wypełniane — zgodnie z wybranym kontem magazynu. Wyświetlana nazwa lokalizacji to `microsoft_azure_[konto magazynu]`, a wybrany poziom dostępu to **Domyślny (hot storage)**. Oba pola można zmodyfikować stosownie do potrzeb.

Uwaga
Zmieniając nazwę lokalizacji, należy wprowadzić unikatową nazwę lokalizacji (nazwa musi być unikatowa w ramach dzierżawcy-klienta). Jeśli dodawana nazwa już występuje na koncie magazynu, rozwiązanie Acronis doda do niej numer jako sufiks. Jeśli więc na przykład występuje już nazwa **Magazyn Microsoft Azure**, zostanie ona automatycznie zmieniona na **Magazyn Microsoft Azure_01**.



6. Kliknij **Dodaj**.

© Acronis International GmbH, 2003-2024

Jeśli tworzysz lub edytujesz plan ochrony, lokalizacja kopii zapasowych Microsoft Azure jest ustawiona jako lokalizacja w wierszu **Miejsce docelowe kopii zapasowej**. Po uruchomieniu operacji tworzenia kopii zapasowej (ręcznie lub zgodnie z harmonogramem) kopia ta jest zapisywana w zdefiniowanej lokalizacji.

Jeśli zarządzasz lokalizacjami magazynów kopii zapasowych, możesz przeglądać i aktualizować szczegóły lokalizacji stosownie do potrzeb. Lokalizacja Microsoft Azure jest też dostępna w przypadku definiowania lokalizacji kopii zapasowych maszyn. Aby uzyskać więcej informacji, zobacz sekcję "Wyświetlanie i aktualizowanie lokalizacji kopii zapasowych w chmurze publicznej" (s. 586).

Definiowanie lokalizacji kopii zapasowych na platformie Amazon S3

Uwaga
Aby móc skonfigurować lokalizacje kopii zapasowych na platformie Amazon S3, trzeba mieć zdefiniowaną jedną z następujących ról w usłudze Cyber Protection: Administrator firmy, Użytkownik, Administrator środowiska cybernetycznego.

Aby móc utworzyć kopię zapasową maszyny na platformie Amazon S3, trzeba zdefiniować lokalizację kopii zapasowych na platformie Amazon S3 w konsoli Cyber Protect, a następnie ustanowić połączenie z odpowiednim połączeniem z Amazon S3. Można to zrobić na następujące sposoby:

- Podczas tworzenia lub edytowania planu ochrony.
- Podczas definiowania lokalizacji magazynów kopii zapasowych i zarządzania nimi.

Ważne
Zarówno administratorzy, jak i użytkownicy niebędący administratorami mogą tworzyć kopie zapasowe maszyn na platformie Amazon S3.

Użytkownicy niebędący administratorami mogą dodawać dostęp do połączenia z Amazon S3 (zobacz sekcję "Zarządzanie dostępem do innych usług chmur publicznych" (s. 595)), ale plany ochrony mogą stosować tylko wtedy, gdy lokalizacja kopii zapasowych jest połączona z tym połączeniem z Amazon S3, które sami dodali, oraz w przypadku maszyn zarejestrowanych w konsoli Cyber Protect przy użyciu ich nazwy użytkownika.

Administratorzy mogą stosować plany ochrony w sytuacji, gdy lokalizacja kopii zapasowych jest połączona z tymi połączeniami z Amazon S3, które sami dodali, lub z subskrypcjami dodanymi przez innego administratora, a także w przypadku maszyn zarejestrowanych w konsoli Cyber Protect w przypadku dowolnego użytkownika.

Aby zdefiniować lokalizację kopii zapasowych na platformie Amazon S3

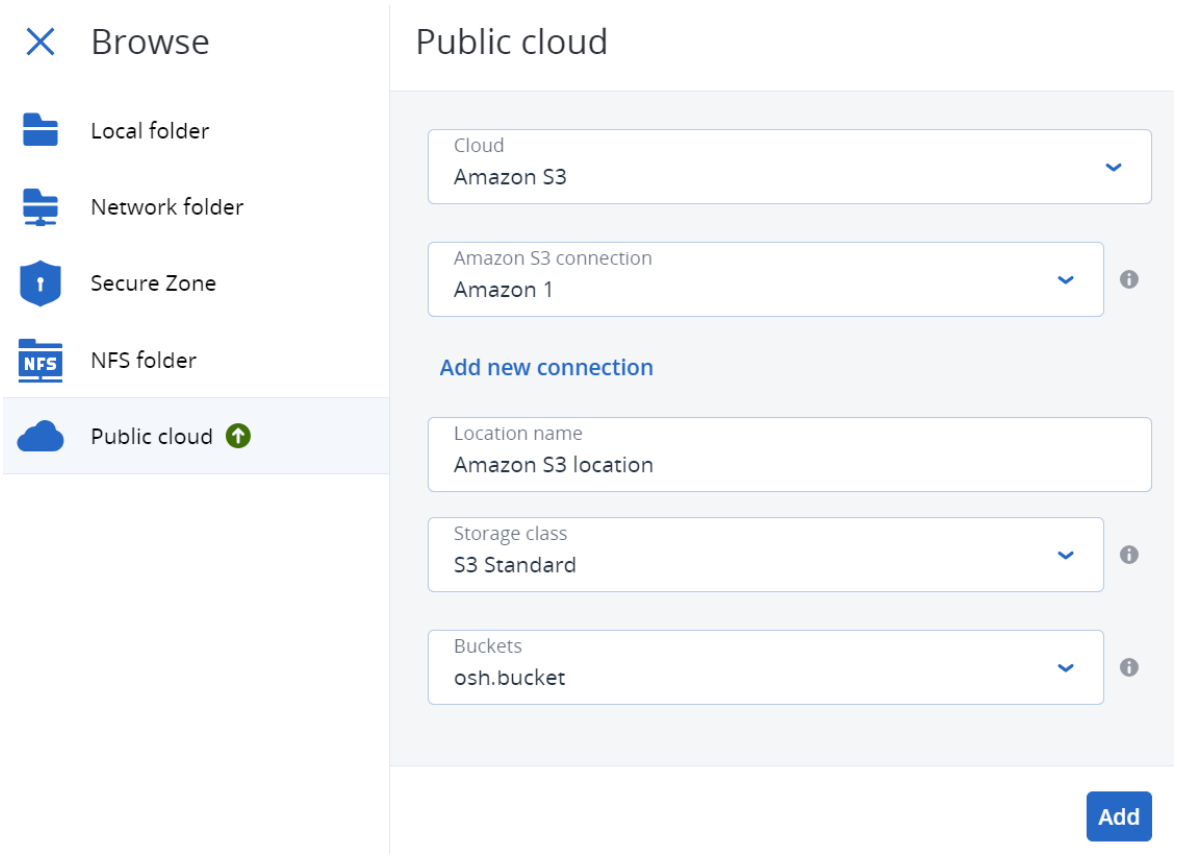
© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect wykonaj jedną z następujących czynności:
   - Jeśli tworzysz lub edytujesz plan ochrony, przejdź do sekcji **Urządzenia**, a następnie wybierz maszynę, której kopię zapasową chcesz utworzyć na platformie Amazon S3. W sekcji **Kopia zapasowa** planu ochrony wybranej maszyny kliknij łącze w wierszu **Miejsce docelowe kopii zapasowej**.

     Dodatkowe informacje na temat pracy z planami ochrony można znaleźć w sekcji "Plany ochrony i moduły" (s. 221).
   - Jeśli zarządzasz lokalizacjami magazynów kopii zapasowych i chcesz dodać Amazon S3 jako nową lokalizację, przejdź do sekcji **Magazyn kopii zapasowych**.

     Dodatkowe informacje na temat zarządzania lokalizacjami magazynów kopii zapasowych można znaleźć w sekcji "Karta Magazyn kopii zapasowych" (s. 566).
2. Kliknij **Dodaj lokalizację**.
3. Z listy rozwijanej **Chmury publiczne** wybierz **Amazon S3**.
4. Jeśli odpowiednie połączenie z Amazon S3 jest już zarejestrowane w konsoli Cyber Protect, wybierz je z listy.

   Jeśli odpowiednie połączenie nie jest zarejestrowane w konsoli Cyber Protect, kliknij **Dodaj nowe połączenie**. Więcej informacji na temat dodawania i definiowania dostępu do połączenia z Amazon S3 można znaleźć w sekcji "Dodawanie dostępu do połączenia z chmurą publiczną" (s. 595). Po dodaniu połączenia przejdź do następnego kroku.



5. Określ następujące opcje:

© Acronis International GmbH, 2003-2024

- W polu **Nazwa lokalizacji** wprowadź nazwę lokalizacji kopii zapasowych.

  Uwaga
  Nazwa lokalizacji musi być unikatowa dla dzierżawcy-klienta. Jeżeli dodana nazwa już istnieje w połączeniu, Acronis doda do nazwy numer jako sufiks. Jeśli na przykład istnieje już **Magazyn Amazon S3**, nazwa zostanie automatycznie zmieniona na **Magazyn Amazon S3 1**.

- W polu **Klasa magazynu** wybierz jedną z następujących obsługiwanych klas magazynów:
  - S3 Standard
  - Standard — rzadki dostęp (S3 Standard-IA)
  - Jedna strefa — rzadki dostęp (S3 One Zone-IA)
  - S3 Intelligent Tiering
- W polu **Zasobnik** wybierz odpowiedni zasobnik platformy Amazon S3.

6. Kliknij **Dodaj**.

   Jeśli tworzysz lub edytujesz plan ochrony, lokalizacja kopii zapasowych na platformie Amazon S3 zostanie ustawiona jako lokalizacja w wierszu **Miejsce docelowe kopii zapasowej**. Po uruchomieniu operacji tworzenia kopii zapasowej (ręcznie lub zgodnie z harmonogramem) kopia zapasowa będzie zapisywana we wskazanej lokalizacji.

   Jeśli zarządzasz lokalizacjami magazynów kopii zapasowych, możesz przeglądać i aktualizować szczegóły lokalizacji stosownie do potrzeb. Lokalizacja Amazon S3 jest też dostępna w przypadku definiowania lokalizacji kopii zapasowych maszyn. Aby uzyskać więcej informacji, zobacz sekcję "Wyświetlanie i aktualizowanie lokalizacji kopii zapasowych w chmurze publicznej" (s. 586).

Definiowanie lokalizacji kopii zapasowych na platformie Wasabi

Uwaga
Aby móc skonfigurować lokalizacje kopii zapasowych na platformie Wasabi, trzeba mieć zdefiniowaną jedną z następujących ról w usłudze Cyber Protection: Administrator firmy, Użytkownik, Administrator środowiska cybernetycznego.

Aby móc utworzyć kopię zapasową maszyny na platformie Wasabi, trzeba zdefiniować lokalizację kopii zapasowych na platformie Wasabi w konsoli Cyber Protect, a następnie ustanowić połączenie z odpowiednim połączeniem z Wasabi. Można to zrobić na następujące sposoby:

- Podczas tworzenia lub edytowania planu ochrony.
- Podczas definiowania lokalizacji magazynów kopii zapasowych i zarządzania nimi.

© Acronis International GmbH, 2003-2024

Ważne
Zarówno administratorzy, jak i użytkownicy niebędący administratorami mogą tworzyć kopie zapasowe maszyn na platformie Wasabi.

Użytkownicy niebędący administratorami mogą dodawać dostęp do połączenia z Wasabi (zobacz sekcję "Zarządzanie dostępem do innych usług chmur publicznych" (s. 595)), ale plany ochrony mogą stosować tylko wtedy, gdy lokalizacja kopii zapasowych jest połączona z tym połączeniem z Wasabi, które sami dodali, oraz w przypadku maszyn zarejestrowanych w konsoli Cyber Protect przy użyciu ich nazwy użytkownika.

Administratorzy mogą stosować plany ochrony w sytuacji, gdy lokalizacja kopii zapasowych jest połączona z tymi połączeniami z Wasabi, które sami dodali, lub z subskrypcjami dodanymi przez innego administratora, a także w przypadku maszyn zarejestrowanych w konsoli Cyber Protect w przypadku dowolnego użytkownika.

Aby zdefiniować lokalizację kopii zapasowych na platformie Wasabi

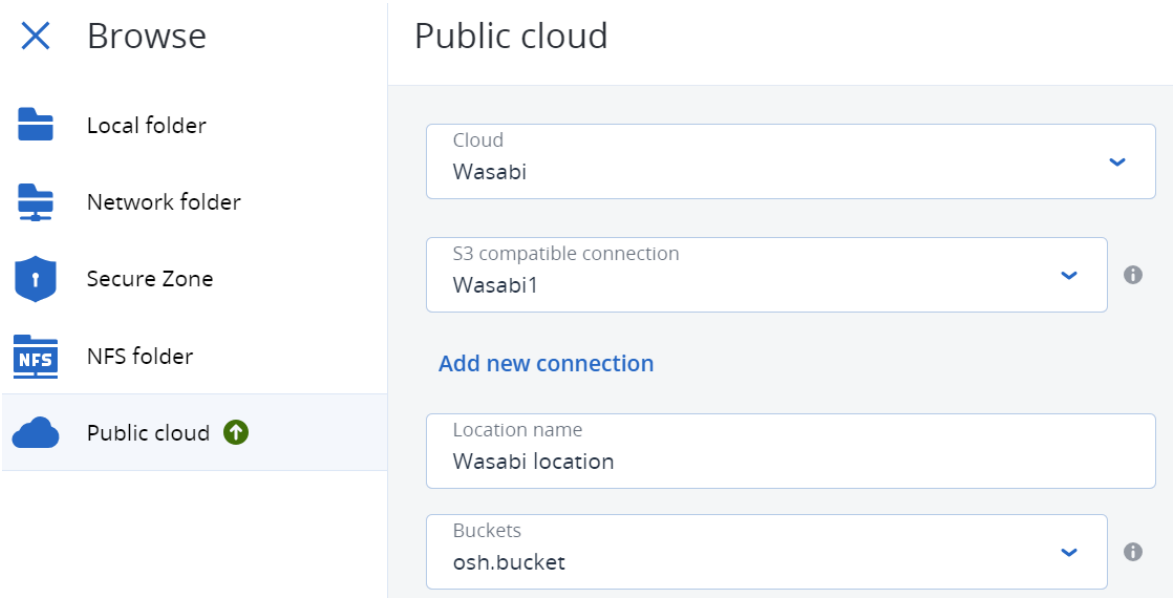
1. W konsoli Cyber Protect wykonaj jedną z następujących czynności:
   - Jeśli tworzysz lub edytujesz plan ochrony, przejdź do sekcji **Urządzenia**, a następnie wybierz maszynę, której kopię zapasową chcesz utworzyć na platformie Wasabi. W sekcji **Kopia zapasowa** planu ochrony wybranej maszyny kliknij łącze w wierszu **Miejsce docelowe kopii zapasowej**.

     Dodatkowe informacje na temat pracy z planami ochrony można znaleźć w sekcji "Plany ochrony i moduły" (s. 221).
   - Jeśli zarządzasz lokalizacjami magazynów kopii zapasowych i chcesz dodać Wasabi jako nową lokalizację, przejdź do sekcji **Magazyn kopii zapasowych**.

     Dodatkowe informacje na temat zarządzania lokalizacjami magazynów kopii zapasowych można znaleźć w sekcji "Karta Magazyn kopii zapasowych" (s. 566).
2. Kliknij **Dodaj lokalizację**.
3. Z listy rozwijanej **Chmury publiczne** wybierz **Wasabi**.
4. Jeśli odpowiednie połączenie z Wasabi jest już zarejestrowane w konsoli Cyber Protect, wybierz je z listy połączeń.

   Jeśli odpowiednie połączenie nie jest zarejestrowane w konsoli Cyber Protect, kliknij **Dodaj nowe połączenie**. Więcej informacji na temat dodawania i definiowania dostępu do połączenia z Wasabi można znaleźć w sekcji "Dodawanie dostępu do połączenia z chmurą publiczną" (s. 595). Po dodaniu połączenia przejdź do następnego kroku.

© Acronis International GmbH, 2003-2024



5. Określ następujące opcje:
   - W polu **Nazwa lokalizacji** wprowadź nazwę lokalizacji kopii zapasowych.

     Uwaga
     Nazwa lokalizacji musi być unikatowa dla dzierżawcy-klienta. Jeżeli dodana nazwa już istnieje w połączeniu, Acronis doda do nazwy numer jako sufiks. Jeśli na przykład istnieje już **Magazyn Wasabi**, nazwa zostanie automatycznie zmieniona na **Magazyn Wasabi 1**.

   - W polu **Zasobnik** wybierz odpowiedni zasobnik platformy Wasabi.
6. Kliknij **Dodaj**.

   Jeśli tworzysz lub edytujesz plan ochrony, lokalizacja kopii zapasowych na platformie Wasabi zostanie ustawiona jako lokalizacja w wierszu **Miejsce docelowe kopii zapasowej**. Po uruchomieniu operacji tworzenia kopii zapasowej (ręcznie lub zgodnie z harmonogramem) kopia zapasowa będzie zapisywana we wskazanej lokalizacji.

   Jeśli zarządzasz lokalizacjami magazynów kopii zapasowych, możesz przeglądać i aktualizować szczegóły lokalizacji stosownie do potrzeb. Lokalizacja Wasabi jest też dostępna w przypadku definiowania lokalizacji kopii zapasowych maszyn. Aby uzyskać więcej informacji, zobacz sekcję "Wyświetlanie i aktualizowanie lokalizacji kopii zapasowych w chmurze publicznej" (s. 586).

Wyświetlanie i aktualizowanie lokalizacji kopii zapasowych w chmurze publicznej

Możesz wyświetlać i aktualizować lokalizacje kopii zapasowych na platformach Microsoft Azure, Amazon S3 i Wasabi zdefiniowane w module **Magazyn kopii zapasowych** lub podczas tworzenia bądź edytowania planu ochrony.

Aby uzyskać informacje na temat usuwania dostępu do subskrypcji Microsoft Azure z konsoli Cyber Protect, zobacz sekcję "Usuwanie dostępu do subskrypcji platformy Microsoft Azure" (s. 594). Aby

© Acronis International GmbH, 2003-2024

uzyskać informacje na temat usuwania dostępu do połączeń z innymi chmurami publicznymi, zobacz sekcję "Zarządzanie dostępem do innych usług chmur publicznych" (s. 595).

Uwaga
Nie można ręcznie odświeżać ani usuwać lokalizacji kopii zapasowych w chmurze publicznej w module **Magazyn kopii zapasowych**. Zawartość lokalizacji kopii zapasowych jest automatycznie aktualizowana po każdej operacji tworzenia kopii zapasowej lub odzyskiwania.

Aby wyświetlić lokalizacje kopii zapasowych w chmurze publicznej

1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych**.
   Zostanie wyświetlona lista lokalizacji kopii zapasowych ze szczegółami dotyczącymi pojemności magazynu i liczby kopii zapasowych przypisanych do danej lokalizacji.
   Dodatkowe informacje na temat pracy z wymienionymi na liście lokalizacjami kopii zapasowych można znaleźć w sekcji "Karta Magazyn kopii zapasowych" (s. 566).
2. Wybierz odpowiednią lokalizację.
   Zostanie wyświetlona lista wszystkich bieżących kopii zapasowych w wybranej lokalizacji.
3. (Opcjonalnie) Kliknij kopię zapasową, aby wyświetlić więcej szczegółów na jej temat.

Aby zaktualizować lokalizację kopii zapasowych w chmurze publicznej w planie ochrony

1. Przejdź do odpowiedniego planu ochrony i wybierz **Edytuj**.
2. Kliknij łącze w wierszu **Miejsce docelowe kopii zapasowej**.
3. Wybierz z listy jedną z istniejących lokalizacji kopii zapasowych lub kliknij **Dodaj lokalizację**, aby dodać nową lokalizację.
   Jeśli odpowiednia subskrypcja Microsoft Azure lub połączenie z chmurą publiczną są już zarejestrowane w konsoli Cyber Protect, wybierz odpowiednią pozycję z wyświetlonej listy.
   Jeśli dodajesz nową subskrypcję Microsoft Azure, pojawi się prośba o uwierzytelnienie danych konta Microsoft (zobacz sekcję "Dodawanie dostępu do subskrypcji platformy Microsoft Azure" (s. 592)). Aby uzyskać więcej informacji na temat wymaganych uprawnień podczas nawiązywania połączenia z platformą Microsoft Azure, zobacz artykuł 72684: Microsoft Azure connection security and audit (Ochrona i inspekcje dotyczące połączeń z platformą Microsoft Azure).

Zarządzanie dostępem do kont w chmurze publicznej

Aby włączyć usługi Acronis Cyber Protection na platformach chmur publicznych, trzeba skonfigurować dostęp do odpowiednich kont w chmurze publicznej.

Na przykład w przypadku pracy z platformą Microsoft Azure wymagany jest dostęp do subskrypcji Microsoft Azure. Po dodaniu subskrypcji w konsoli Cyber Protect można ją wybrać podczas konfigurowania bezpośredniej kopii zapasowej na platformie Microsoft Azure. Podobnie w przypadku pracy z platformą Amazon S3 lub Wasabi wymagane są odpowiednie klucze dostępu powiązane z określonymi zasadami dotyczącymi tworzenia kopii zapasowych.

© Acronis International GmbH, 2003-2024

Dostępem do chmur publicznych zarządza się za pośrednictwem menu **Infrastruktura** w konsoli Cyber Protect.

Ważne
Sprawdzanie poprawności kopii zapasowych jest wyłączone w przypadku kopii zapasowych w chmurze publicznej, aby uniknąć nadmiernych kosztów ruchu wychodzącego. Ponadto obecnie nie można „ponownie podłączyć" lokalizacji kopii zapasowych w chmurze publicznej do tego samego lub innego dzierżawcy klienta, jeśli lokalizacja została wcześniej usunięta. Aby uzyskać więcej informacji, skontaktuj się z zespołem pomocy technicznej.

Wymagania dotyczące dostępu potrzebnego do tworzenia kopii zapasowych w chmurze publicznej

W przypadku bezpośredniego tworzenia kopii zapasowych w usługach chmury publicznej należy wziąć pod uwagę szereg wymagań dotyczących dostępu w kontekście każdej platformy:

- Microsoft Azure
- Amazon S3
- Wasabi

Tworzenie kopii zapasowych na platformie Microsoft Azure

Aby nawiązać połączenie z subskrypcją Microsoft Azure, musisz mieć różne uprawnienia. Dodatkowe informacje na ich temat można znaleźć w artykule 72684 Microsoft Azure connection security and audit (Ochrona i inspekcja połączeń z Microsoft Azure).

Uwaga
Aby ukończyć połączenie z subskrypcją, musisz mieć przypisaną jedną z następujących ról w usłudze Microsoft Azure AD: Administrator aplikacji w chmurze, Administrator aplikacji lub Administrator globalny. Musisz też mieć przypisaną rolę właściciela w przypadku każdej wybranej subskrypcji.

Tworzenie kopii zapasowych na platformie Amazon S3

W przypadku tworzenia kopii zapasowych na platformie Amazon S3 podczas definiowania lokalizacji kopii zapasowych na platformie Amazon S3 musi zostać spełnionych kilka wymagań:

- Obsługiwane klasy magazynów
- Uprawnienia związane z zasadami
- Klucze dostępu
- Ustawienia dotyczące zasobników

Obsługiwane klasy magazynów

Obecnie obsługiwane są następujące klasy magazynów na platformie Amazon S3:

© Acronis International GmbH, 2003-2024

- S3 Standard
- Standard — rzadki dostęp (S3 Standard-IA)
- Jedna strefa — rzadki dostęp (S3 One Zone-IA)
- S3 Intelligent Tiering

Uprawnienia związane z zasadami

W przypadku tworzenia kopii zapasowych na platformie Amazon S3 Twoje konto Amazon musi mieć zastosowane minimalne uprawnienia, aby rozwiązanie Acronis mogło tworzyć kopie zapasowe odpowiednich maszyn na platformie Amazon S3. Oznacza to, że odpowiedni użytkownicy powinni mieć dostęp do konsoli AWS Management Console, a do grup, do których są przypisani, powinny być zastosowane odpowiednie zasady.

Przykłady

Poniższe przykładowe zasady odzwierciedlają minimalny zestaw uprawnień do szerokiej puli zasobów. Uwaga: `*` oznacza wszystkie zasoby.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource": "*" },
{ "Effect": "Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, {
"Effect": "Allow", "Action": [ "s3:GetBucketLocation", "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:ListBucket" ], "Resource": "*" } ] }
```

Poniższe przykładowe zasady odzwierciedlają minimalne uprawnienia ograniczone do określonego zasobnika. Uwaga: zmienną `[BUCKETNAME]` należy zastąpić nazwą zasobnika.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource":
"arn:aws:s3:::[BUCKETNAME]" }, { "Effect": "Allow", "Action":
"sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect": "Allow", "Action": [
"s3:ListBucket" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Klucze dostępu

Klucze dostępu są wymagane przez firmę Acronis w przypadku każdego połączenia z platformą Amazon S3 i są używane podczas definiowania połączenia z platformą Amazon S3. Więcej informacji na temat generowania kluczy dostępu i identyfikatorów kluczy dostępu można znaleźć w dokumentacji platformy Amazon S3.

© Acronis International GmbH, 2003-2024

Ustawienia dotyczące zasobników

Jeśli używasz zasobników platformy Amazon S3 jako lokalizacji kopii zapasowych, upewnij się, że zasobnik ma skonfigurowane ustawienia domyślne, w tym blokowanie wszelkiego dostępu publicznego (domyślnie jest to ustawione jako **Wł.**). Więcej informacji na temat pracy z zasobnikami można znaleźć w dokumentacji platformy Amazon S3.

Uwaga
Acronis obecnie nie obsługuje przechowywania wersji zasobników ani blokowania obiektów na platformie Amazon S3, nawet jeśli funkcje te są włączone w przypadku danego zasobnika.

Tworzenie kopii zapasowych na platformie Wasabi

W przypadku tworzenia kopii zapasowych na platformie Wasabi podczas definiowania lokalizacji kopii zapasowych należy uwzględnić szereg wymagań:

- Uprawnienia związane z zasadami
- Klucze dostępu
- Ustawienia dotyczące zasobników

Uprawnienia związane z zasadami

Definiując lokalizację kopii zapasowych na platformie Wasabi, należy się upewnić, że odpowiednie zasady są stosowane do odpowiednich grup i użytkowników w środowisku Wasabi.

Przykłady

Poniższe przykładowe zasady odzwierciedlają minimalny zestaw uprawnień do szerokiej puli zasobów. Uwaga: * oznacza dowolny zasób.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "*" }, { "Effect": "Allow", "Action": [
"iam:CreateRole", "iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole"
], "Resource": "*" }, { "Effect": "Allow", "Action": [ "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": "s3:ListBucket", "Resource": "*" } ] }
```

Poniższe przykładowe zasady przedstawiają ograniczone uprawnienia w odniesieniu do ograniczonej puli zasobów. Pamiętaj, że zmienną `[BUCKETNAME]` należy zastąpić nazwą zasobnika, a zmienną `[ACCOUNTID]` identyfikatorem konta na platformie Wasabi.

© Acronis International GmbH, 2003-2024

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect":
"Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Klucze dostępu

Klucze dostępu są wymagane przez firmę Acronis w przypadku każdego połączenia z platformą Wasabi i używane podczas definiowania połączenia z platformą Wasabi.

Należy pamiętać, że klucze dostępu do kont użytkowników root na platformie Wasabi nie mogą być używane, ponieważ użytkownicy root nie mogą wywoływać funkcji AssumeRole. Należy utworzyć osobnego użytkownika niebędącego użytkownikiem root i wygenerować dla niego klucze dostępu.

Więcej informacji na temat generowania kluczy dostępu i identyfikatorów kluczy dostępu można znaleźć w dokumentacji platformy Wasabi.

Ustawienia dotyczące zasobników

Jeśli używasz zasobników Wasabi jako lokalizacji kopii zapasowych, upewnij się, że dany zasobnik ma skonfigurowane ustawienia domyślne. Więcej informacji na temat pracy z zasobnikami można znaleźć w dokumentacji platformy Wasabi.

Uwaga
Acronis obecnie nie obsługuje przechowywania wersji zasobników ani blokowania obiektów na platformie Wasabi, nawet jeśli funkcje te są włączone w przypadku danego zasobnika.

Zarządzanie dostępem do subskrypcji platformy Microsoft Azure

Dzięki ustanowieniu połączenia z odpowiednimi subskrypcjami platformy Microsoft Azure w konsoli Cyber Protect można tworzyć kopie zapasowe odpowiednich obciążeń bezpośrednio na platformie Microsoft Azure.

Połączenie z subskrypcją można skonfigurować podczas tworzenia lokalizacji kopii zapasowych za pomocą menu **Urządzenia** lub **Magazyn kopii zapasowych**, zgodnie z opisem podanym w sekcji "Definiowanie lokalizacji kopii zapasowych na platformie Microsoft Azure" (s. 579).

Ewentualnie te subskrypcje platformy Microsoft Azure można skonfigurować na ekranie **Chmury publiczne** (kliknij **Infrastruktura > Chmury publiczne**). W tym miejscu można też zarządzać subskrypcjami, m.in. odnawiać dostęp do subskrypcji, przeglądać właściwości i działania subskrypcji lub usuwać subskrypcje.

© Acronis International GmbH, 2003-2024

W zależności od przypisanej roli użytkownika możesz mieć możliwość zarządzania subskrypcjami Microsoft Azure dodanymi przez innych użytkowników w ramach swojej organizacji. Jeśli na przykład jesteś administratorem firmy lub jednostki albo przypisano Ci rolę administratora środowiska cybernetycznego lub administratora w usłudze Cyber Protection, możesz przeglądać subskrypcje Microsoft Azure dodane przez innych administratorów i subskrypcje dodane przez użytkowników niebędących administratorami oraz nimi zarządzać. Użytkownicy niebędący administratorami mogą wyświetlać tylko te subskrypcje Microsoft Azure, które dodali do konsoli Cyber Protect, i tylko do nich uzyskiwać dostęp.

Uwaga
Partnerzy mogą zarządzać subskrypcjami platformy Microsoft Azure klientów znajdujących się poniżej ich poziomu w hierarchii. Jeśli jednak partner wybierze opcję **Wszyscy klienci**, menu **Infrastruktura** w konsoli Cyber Protect nie będzie dostępne.

Ważne
Podczas nawiązywania połączenia z subskrypcją platformy Microsoft Azure rozwiązanie Acronis wymaga minimalnych uprawnień. Dodatkowe informacje na temat wymaganych uprawnień można znaleźć w artykule 72684: Microsoft Azure connection security and audit (Bezpieczeństwo i audyt połączenia z platformą Microsoft Azure).

Dodawanie dostępu do subskrypcji platformy Microsoft Azure

Dzięki dodaniu subskrypcji platformy Microsoft Azure w konsoli Cyber Protect rozwiązanie Acronis może bezpiecznie uzyskiwać dostęp do subskrypcji i tworzyć kopie zapasowe odpowiednich obciążeń bezpośrednio na platformie Microsoft Azure.

Aby dodać dostęp do subskrypcji platformy Microsoft Azure

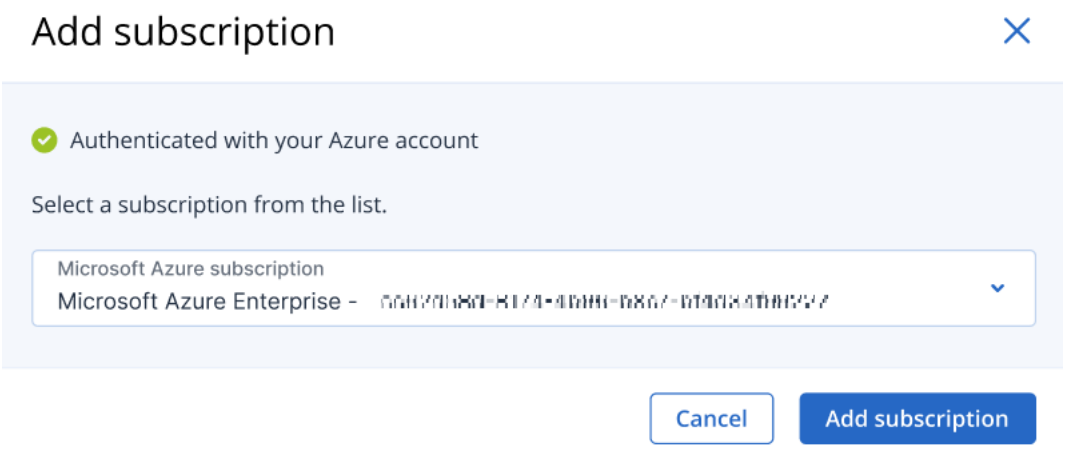
1. W konsoli Cyber Protect przejdź do sekcji **Infrastruktura > Chmury publiczne**.
2. Kliknij **Dodaj** i z wyświetlonej listy opcji wybierz **Microsoft Azure**.
3. W wyświetlonym oknie dialogowym kliknij **Zaloguj się**. Nastąpi przekierowanie do strony logowania Microsoft.

   Uwaga
   Aby ukończyć połączenie z subskrypcją, musisz mieć przypisaną jedną z następujących ról w usłudze Microsoft Azure AD: Administrator aplikacji w chmurze, Administrator aplikacji lub Administrator globalny. Musisz też mieć przypisaną rolę właściciela w przypadku każdej wybranej subskrypcji.

4. Na ekranie logowania na koncie Microsoft wprowadź swoje dane logowania i zaakceptuj wymagane uprawnienia. Rozpocznie się proces łączenia, który może potrwać kilka minut.
   Dodatkowe informacje na temat bezpiecznego uzyskiwania dostępu do platformy Microsoft Azure i subskrypcji można znaleźć w artykule 72684: Microsoft Azure connection security and audit (Bezpieczeństwo i audyt połączenia z platformą Microsoft Azure).

© Acronis International GmbH, 2003-2024

5. Po ustanowieniu połączenia wybierz odpowiednią subskrypcję z listy rozwijanej w wyświetlonym oknie dialogowym i kliknij **Dodaj subskrypcję**.



Subskrypcja zostanie dodana do listy chmur publicznych.

Jeśli chcesz odnowić roczny certyfikat dostępu do subskrypcji, zobacz sekcję "Odnawianie dostępu do subskrypcji platformy Microsoft Azure" (s. 593).

Jeśli chcesz usunąć dostęp do subskrypcji, zobacz sekcję "Usuwanie dostępu do subskrypcji platformy Microsoft Azure" (s. 594).

Uwaga
Jeśli konto Microsoft Azure, na którym się zalogowano, obejmuje dostęp do wielu usług Microsoft Azure AD, w tym usług AD, w których zaproszono Cię jako użytkownika-gościa, zostanie wybrany tylko domyślny katalog użytkownika. Aby skorzystać z katalogu, w którym jesteś użytkownikiem-gościem, musisz utworzyć nowego użytkownika w danej usłudze Microsoft Azure AD. Następnie możesz się zalogować na tym koncie i połączyć z odpowiednią subskrypcją.

Odnawianie dostępu do subskrypcji platformy Microsoft Azure

Po rejestracji w konsoli Cyber Protect dostęp do subskrypcji platformy Microsoft Azure jest konfigurowany automatycznie na rok — rozwiązanie Acronis korzysta z bezpłatnego unikatowego certyfikatu dostępu. Gdy zbliża się data wygaśnięcia certyfikatu, można go szybko i łatwo odnowić.

Aby odnowić certyfikat dostępu do subskrypcji platformy Microsoft Azure

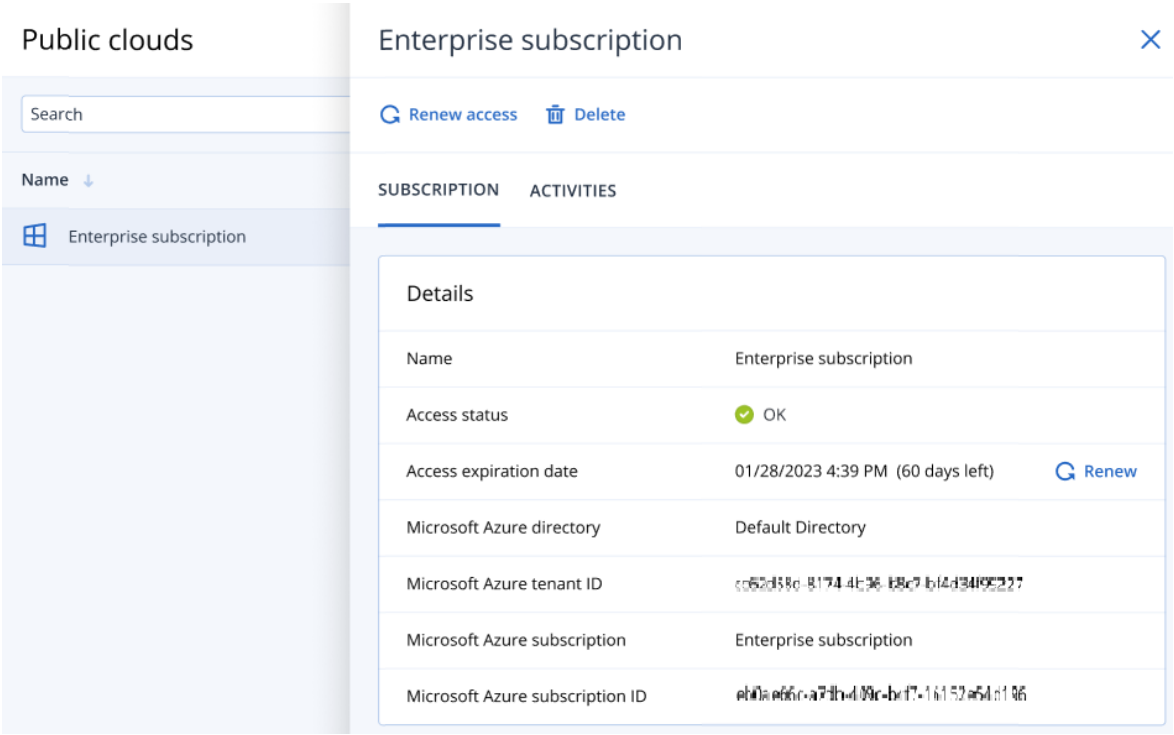
1. W konsoli Cyber Protect przejdź do sekcji **Infrastruktura > Chmury publiczne**.
2. Wybierz odpowiednią subskrypcję z wyświetlonej listy.

   Uwaga
   W kolumnie **Status dostępu** jest wskazywany bieżący status certyfikatu dostępu dla każdej subskrypcji, a jest to jeden z dwóch statusów: **OK** lub **Wygasł**.

3. W prawym panelu kliknij **Odnów dostęp**.

   Możesz też kliknąć kartę **Subskrypcja**, a następnie kliknąć **Odnów** w polu **Data wygaśnięcia dostępu**.

© Acronis International GmbH, 2003-2024



4. Na ekranie logowania na koncie Microsoft wprowadź swoje dane logowania i zaakceptuj wymagane uprawnienia. Rozpocznie się proces łączenia, który może potrwać kilka minut.
   Po pomyślnym uwierzytelnieniu dostęp zostanie automatycznie odnowiony na rok.
   Dodatkowe informacje na temat wymaganych uprawnień można znaleźć w artykule 72684: Microsoft Azure connection security and audit (Bezpieczeństwo i audyt połączenia z platformą Microsoft Azure).

Usuwanie dostępu do subskrypcji platformy Microsoft Azure

Jeśli nie tworzysz kopii zapasowych obciążeń na platformie Microsoft Azure, warto usunąć dostęp do subskrypcji platformy Microsoft Azure.

Aby usunąć dostęp do subskrypcji platformy Microsoft Azure

Ważne
Jeśli subskrypcja jest aktualnie używana do tworzenia kopii zapasowych na platformie Microsoft Azure, nie można jej usunąć.

1. W konsoli Cyber Protect przejdź do sekcji **Infrastruktura > Chmury publiczne**.
2. Wybierz odpowiednią subskrypcję z wyświetlonej listy.
3. W prawym panelu kliknij **Usuń**.

Uwaga
Możesz usunąć tylko dodaną przez siebie subskrypcję. Subskrypcję możesz też usunąć, jeśli jesteś administratorem firmy lub administratorem jednostki albo przypisano Ci rolę administratora środowiska cybernetycznego lub administratora w usłudze Cyber Protection.

© Acronis International GmbH, 2003-2024

4. W wyświetlonym komunikacie dotyczącym potwierdzenia kliknij **Usuń**.

Zarządzanie dostępem do innych usług chmur publicznych

Uwaga
Ta sekcja odnosi się do zarządzania dostępem do wszystkich usług chmur publicznych innych niż Microsoft Azure, którą opisano w sekcji "Zarządzanie dostępem do subskrypcji platformy Microsoft Azure" (s. 591).

Jeśli w konsoli Cyber Protect ustanowisz połączenie z odpowiednim kontem w chmurze publicznej, zyskasz możliwość tworzenia kopii zapasowych maszyn bezpośrednio w odpowiedniej chmurze publicznej.

Połączenia z kontami w chmurze publicznej możesz skonfigurować podczas tworzenia lokalizacji kopii zapasowych za pomocą menu **Urządzenia** lub **Magazyn kopii zapasowych**. Możesz też skonfigurować połączenia z chmurą publiczną na ekranie **Chmury publiczne** (wybierz kolejno **Infrastruktura > Chmury publiczne**). W tym miejscu możesz też zarządzać swoim połączeniem, w tym odnowić dostęp do połączenia, przejrzeć właściwości i działanie połączenia lub usunąć połączenie.

W zależności od przypisanej roli użytkownika możesz mieć możliwość zarządzania połączeniami z chmurą publiczną dodanymi przez innych użytkowników z Twojej organizacji. Jeśli na przykład jesteś administratorem firmy lub jednostki albo przypisano Ci rolę administratora środowiska cybernetycznego bądź administratora w usłudze Cyber Protection, możesz przeglądać połączenia z chmurą publiczną dodane przez innych administratorów, a także połączenia dodane przez użytkowników niebędących administratorami, i nimi zarządzać. Użytkownicy niebędący administratorami mogą przeglądać tylko te połączenia z chmurą publiczną, które dodali do konsoli Cyber Protect, i tylko do nich mają dostęp.

Uwaga
Partnerzy mogą zarządzać połączeniami klientów z chmurą publiczną poniżej ich poziomu w hierarchii. Jeśli jednak partner wybierze opcję **Wszyscy klienci**, menu **Infrastruktura** w konsoli Cyber Protect nie będzie dostępne.

Ważne
Podczas nawiązywania połączenia z chmurą publiczną, Acronis wymaga szeregu uprawnień. Aby uzyskać więcej informacji, zobacz sekcję "Wymagania dotyczące dostępu potrzebnego do tworzenia kopii zapasowych w chmurze publicznej" (s. 588).

Dodawanie dostępu do połączenia z chmurą publiczną

Po dodaniu połączenia z chmurą publiczną (taką jak Amazon S3 czy Wasabi) w konsoli Cyber Protect Acronis może bezpiecznie uzyskiwać dostęp do zasobów w chmurze i bezpośrednio tworzyć kopie zapasowe maszyn w odpowiedniej chmurze publicznej.

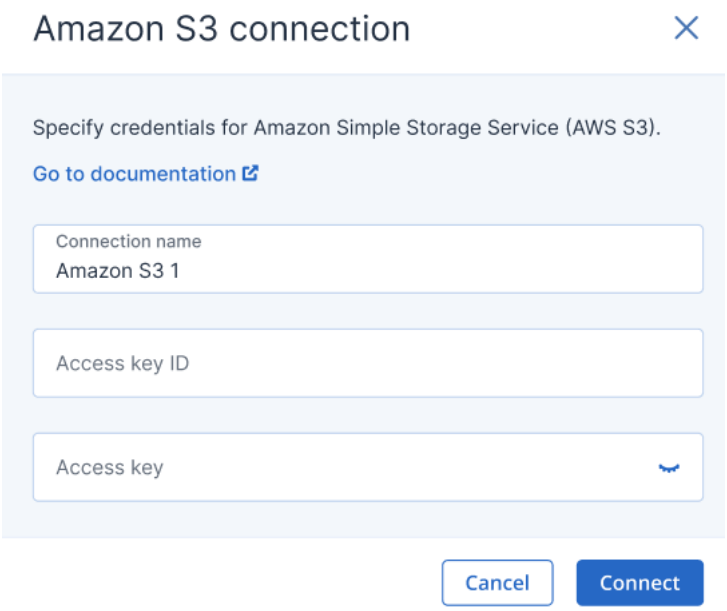
Aby dodać dostęp do połączenia z chmurą publiczną

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Infrastruktura > Chmury publiczne**.
2. Kliknij **Dodaj** i wybierz jedną z następujących opcji:
   - **Amazon S3**

     W wyświetlonym oknie dialogowym zdefiniuj następujące elementy:
     - **Nazwa połączenia**: nazwa połączenia z Amazon S3.
     - **Identyfikator klucza dostępu**: identyfikator klucza dostępu użytkownika do usługi Amazon S3.
     - **Klucz dostępu**: klucz dostępu użytkownika do usługi Amazon S3.

       Klucz dostępu i identyfikator klucza dostępu umożliwiają firmie Acronis uzyskiwanie dostępu do klas oraz zasobników pamięci masowej w ramach odpowiedniego połączenia. Aby uzyskać więcej informacji na temat kluczy i uprawnień dostępu wymaganych przez rozwiązanie Acronis, zobacz sekcję "Wymagania dotyczące dostępu potrzebnego do tworzenia kopii zapasowych w chmurze publicznej" (s. 588).

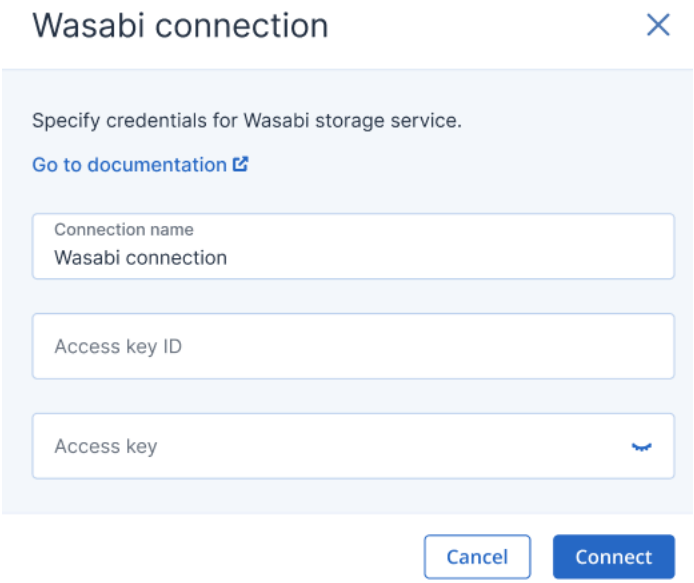
   - **Wasabi**

     W wyświetlonym oknie dialogowym zdefiniuj następujące elementy:
     - **Nazwa połączenia**: nazwa połączenia z usługą Wasabi.
     - **Identyfikator klucza dostępu**: identyfikator klucza dostępu użytkownika na potrzeby usługi Wasabi.
     - **Klucz dostępu**: klucz dostępu użytkownika na potrzeby usługi Wasabi.

       Klucz dostępu i identyfikator klucza dostępu umożliwiają firmie Acronis uzyskiwanie dostępu do klas oraz zasobników pamięci masowej w ramach odpowiedniego połączenia. Aby uzyskać więcej informacji na temat kluczy i uprawnień dostępu wymaganych przez rozwiązanie Acronis, zobacz sekcję "Wymagania dotyczące dostępu potrzebnego do

© Acronis International GmbH, 2003-2024

tworzenia kopii zapasowych w chmurze publicznej" (s. 588).



3. Kliknij **Połącz**.

   Rozpocznie się proces nawiązywania połączenia, który może potrwać kilka minut. Po zakończeniu połączenie zostanie dodane do listy chmur publicznych.

   Jeśli chcesz odnowić roczny certyfikat dostępu na potrzeby danego połączenia, zobacz sekcję "Odnawianie dostępu do połączenia z chmurą publiczną" (s. 597).

   Jeśli chcesz usunąć dostęp na potrzeby danego połączenia, zobacz sekcję "Usuwanie dostępu do połączenia z chmurą publiczną" (s. 598).

Odnawianie dostępu do połączenia z chmurą publiczną

Po zarejestrowaniu połączenia z chmurą publiczną w konsoli Cyber Protect Acronis automatycznie przypisuje bezpłatny i unikatowy certyfikat dostępu, który umożliwia uzyskanie dostępu do połączenia z chmurą publiczną. Certyfikat jest ważny przez rok. Gdy zbliża się data wygaśnięciu certyfikatu, można go odnowić.

Aby odnowić certyfikat dostępu na potrzeby połączenia z chmurą publiczną

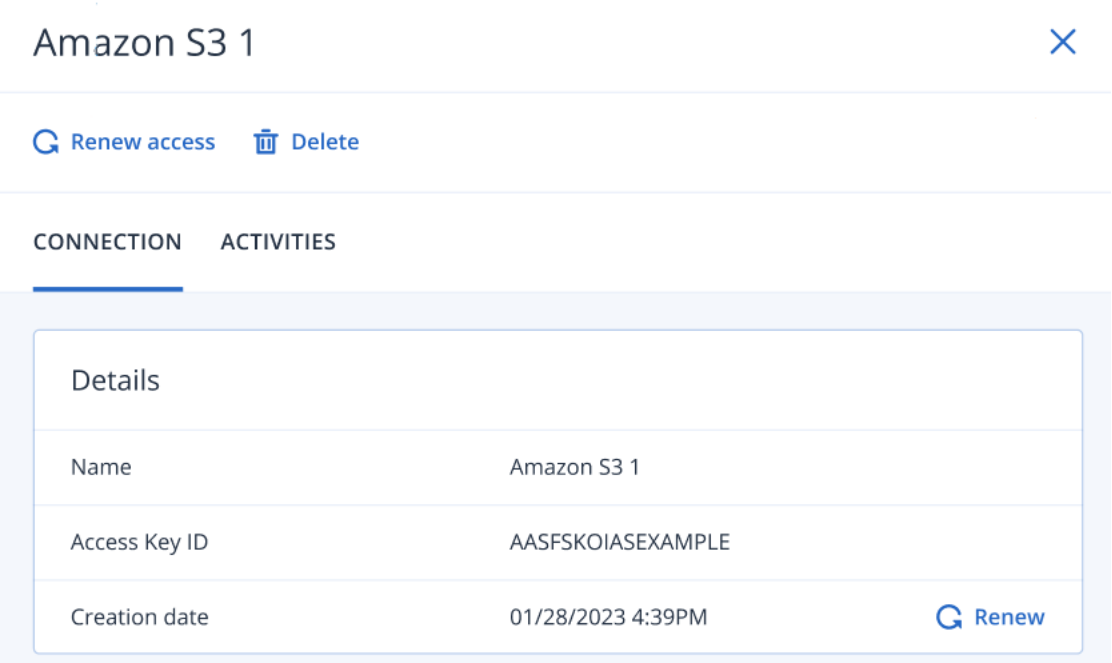
1. W konsoli Cyber Protect przejdź do sekcji **Infrastruktura > Chmury publiczne**.
2. Wybierz odpowiednie połączenie z listy.

   Uwaga
   Kolumna **Status dostępu** wskazuje bieżący status certyfikatu dostępu dla każdego połączenia i wyświetla jeden z dwóch statusów: **OK** lub **Wygasło**.

3. W prawym panelu kliknij **Odnów dostęp**.

   Możesz też kliknąć kartę **Połączenie**, a następnie kliknąć **Odnów** w wierszu **Data utworzenia**.

© Acronis International GmbH, 2003-2024



Po pomyślnym uwierzytelnieniu dostęp zostanie automatycznie odnowiony na rok.

Usuwanie dostępu do połączenia z chmurą publiczną

Jeśli nie tworzysz kopii zapasowych maszyn w chmurach publicznych, lepiej usuń dostęp do połączeń z chmurami publicznymi.

Aby usunąć dostęp do połączenia z chmurą publiczną

Ważne
Nie można usunąć połączenia, jeśli jest ono używane do tworzenia kopii zapasowych w chmurze publicznej.

1. W konsoli Cyber Protect przejdź do sekcji **Infrastruktura > Chmury publiczne**.
2. Wybierz połączenie z listy.
3. W prawym panelu kliknij **Usuń**.

   Uwaga
   Możesz usunąć tylko dodane przez siebie połączenie. Połączenie możesz też usunąć, jeśli jesteś administratorem firmy lub administratorem jednostki albo przypisano Ci rolę administratora środowiska cybernetycznego lub administratora w usłudze Cyber Protection.

4. W wyświetlonym komunikacie dotyczącym potwierdzenia kliknij **Usuń**.

© Acronis International GmbH, 2003-2024

Ochrona aplikacji firmy Microsoft

Chronienie programów Microsoft SQL Server i Microsoft Exchange Server

Uwaga
Kopie zapasowe Microsoft SQL są obsługiwane tylko w przypadku baz danych działających w systemach plików NFTS, REFS i FAT32. System plików ExFat nie jest obsługiwany.

Dostępne są dwie metody ochrony aplikacji firmy Microsoft:

- **Kopia zapasowa bazy danych**
  Jest to kopia zapasowa na poziomie plików uwzględniająca bazy danych oraz powiązane z nimi metadane. Bazy danych można odzyskać do działających aplikacji lub jako pliki.
- **Kopia zapasowa uwzględniająca aplikacje**
  Jest to kopia zapasowa na poziomie dysku, która gromadzi również metadane aplikacji. Metadane te umożliwiają przeglądanie i odzyskiwanie danych aplikacji bez odzyskiwania całego dysku lub woluminu. Możliwe jest również odzyskanie całego dysku lub woluminu. Dzięki temu można używać jednego rozwiązania i jednego planu ochrony do odzyskiwania po awarii oraz ochrony danych.

W przypadku programu Microsoft Exchange Server możesz wybrać **kopię zapasową skrzynki pocztowej**. Jest to kopia zapasowa indywidualnych skrzynek pocztowych za pośrednictwem protokołu Usługi sieci Web programu Exchange. Skrzynki pocztowe lub elementy skrzynek pocztowych można odzyskać na aktywny serwer Exchange Server lub do usługi Microsoft 365. Kopia zapasowa skrzynki pocztowej jest obsługiwana w przypadku programu Microsoft Exchange Server 2010 z dodatkiem Service Pack 1 (SP1) lub nowszego.

Ochrona programu Microsoft SharePoint

Farma programu Microsoft SharePoint zawiera serwery frontonu z działającymi usługami programu SharePoint, serwery baz danych z uruchomionym programem Microsoft SQL Server oraz (opcjonalnie) serwery aplikacji, które odciążają serwery typu frontonu, przejmując część usług programu SharePoint. Niektóre serwery frontonu i serwery aplikacji mogą być identyczne.

Aby chronić całą farmę programu SharePoint:

- Utwórz kopię zapasową wszystkich serwerów baz danych przy użyciu kopii zapasowej uwzględniającej aplikacje.
- Utwórz kopię zapasową wszystkich unikatowych serwerów frontonu i serwerów aplikacji przy użyciu zwykłej kopii zapasowej na poziomie dysku.

Kopie zapasowe wszystkich serwerów powinny zostać utworzone na podstawie tego samego harmonogramu.

© Acronis International GmbH, 2003-2024

Aby chronić tylko zawartość, można osobno utworzyć kopie zapasowe baz danych zawartości.

Chronienie kontrolera domeny

Komputer z uruchomionymi usługami domenowymi Active Directory można chronić przy użyciu kopii zapasowej uwzględniającej aplikacje. Jeśli domena zawiera więcej niż jeden kontroler domeny i jeden z nich zostanie odzyskany, wykonywane jest przywracanie nieautorytatywne i po odzyskaniu nie nastąpi wycofanie numeru USN.

Odzyskiwanie aplikacji

W poniższej tabeli zestawiono dostępne metody odzyskiwania aplikacji.

	Z kopii zapasowej baz danych	**Z kopii zapasowej uwzględniającej aplikacje**	**Z kopii zapasowej dysku**
Microsoft SQL Server	Bazy danych do działającej instancji SQL Server Bazy danych jako pliki	Cały komputer Bazy danych do działającej instancji SQL Server Bazy danych jako pliki	Cały komputer
Microsoft Exchange Server	Bazy danych do działającego programu Exchange Bazy danych jako pliki Odzyskiwanie granularne na aktywny serwer Exchange lub do usługi Microsoft 365*	Cały komputer Bazy danych do działającego programu Exchange Bazy danych jako pliki Odzyskiwanie granularne na aktywny serwer Exchange lub do usługi Microsoft 365*	Cały komputer
Serwery baz danych programu Microsoft SharePoint	Bazy danych do działającej instancji SQL Server Bazy danych jako pliki Odzyskiwanie granularne przy użyciu programu SharePoint Explorer	Cały komputer Bazy danych do działającej instancji SQL Server Bazy danych jako pliki Odzyskiwanie granularne przy użyciu programu SharePoint Explorer	Cały komputer
Internetowe serwery frontonu programu Microsoft SharePoint	-	-	Cały komputer
Usługi domenowe Active Directory	-	Cały komputer	-

© Acronis International GmbH, 2003-2024

* Odzyskiwanie granularne jest również dostępne dla kopii zapasowych skrzynek pocztowych. Odzyskiwanie elementów danych programu Exchange do usługi Microsoft 365 i na odwrót jest obsługiwane pod warunkiem, że lokalnie jest zainstalowany agent dla usługi Microsoft 365.

Wymagania wstępne

Przed skonfigurowaniem kopii zapasowej aplikacji dopilnuj, aby zostały spełnione niżej wymienione wymagania.

Aby sprawdzić stan składników zapisywania usługi VSS, skorzystaj z polecenia `vssadmin list writers`.

Typowe wymagania

W przypadku programu Microsoft SQL Server upewnij się, że:

- Jest uruchomiona co najmniej jedna instancja programu Microsoft SQL Server.
- Jest włączony moduł zapisujący SQL dla usługi VSS.

W przypadku programu Microsoft Exchange Server upewnij się, że:

- Jest uruchomiona usługa Magazyn informacji programu Microsoft Exchange.
- Jest zainstalowane oprogramowanie Windows PowerShell. W przypadku programu Exchange 2010 lub nowszego wymagane jest oprogramowanie Windows PowerShell w wersji 2.0 lub nowszej.
- Jest zainstalowane oprogramowanie Microsoft .NET Framework.

  W przypadku programu Exchange 2007 wymagane jest oprogramowanie Windows .NET Framework w wersji 2.0 lub nowszej.

  W przypadku programu Exchange 2010 lub nowszego wymagane jest oprogramowanie Windows .NET Framework w wersji 3.5 bądź nowszej.
- Moduł zapisujący programu Exchange dla usługi VSS jest włączony.

Uwaga
Agent dla programu Exchange potrzebuje do działania tymczasowego magazynu. Domyślnie pliki tymczasowe są umieszczane w folderze `%ProgramData%\Acronis\Temp`. Ilość wolnego miejsca na woluminie, na którym znajduje się folder `%ProgramData%`, musi wynosić co najmniej 15 procent rozmiaru bazy danych programu Exchange. Przed rozpoczęciem tworzenia kopii zapasowych programu Exchange można też zmienić lokalizację plików tymczasowych zgodnie z opisem podanym w artykule Zmienianie lokalizacji tymczasowych plików i folderów (40040).

Na kontrolerze domeny upewnij się, że:

- Jest włączony moduł zapisujący Active Directory dla usługi VSS.

Tworząc plan ochrony, upewnij się, że:

© Acronis International GmbH, 2003-2024

- W przypadku komputerów fizycznych i maszyn wirtualnych z zainstalowanym agentem jest włączona opcja tworzenia kopii zapasowych Usługa kopiowania woluminów w tle (VSS).
- W przypadku maszyn wirtualnych jest włączona opcja tworzenia kopii zapasowych Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych.

Dodatkowe wymagania dotyczące kopii zapasowych uwzględniających aplikacje

Podczas tworzenia planu ochrony dopilnuj, aby dla kopii zapasowej została wybrana opcja **Cały komputer**. W planie ochrony musi być wyłączona opcja tworzenia kopii zapasowych **Sektor po sektorze**. W przeciwnym razie nie będzie można odzyskać danych aplikacji z kopii zapasowych utworzonych w tym trybie. Odzyskanie danych aplikacji nie będzie możliwe również w przypadku wykonania planu w trybie **Sektor po sektorze** w wyniku automatycznego włączenia tego trybu.

Wymagania dotyczące maszyn wirtualnych ESXi

Jeśli aplikacja działa na maszynie wirtualnej, której kopie zapasowe tworzy agent dla VMware, upewnij się, że:

- Maszyna wirtualna uwzględniana w kopii zapasowej spełnia wymagania wyciszenia spójnego z aplikacjami wymienione w artykule „Windows Backup Implementations" (Implementacje funkcji kopii zapasowych systemu Windows) w dokumentacji rozwiązania VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- Na maszynie są zainstalowane aktualne narzędzia VMware Tools.
- Na maszynie jest wyłączona usługa kontroli konta użytkownika (UAC). Jeśli nie chcesz wyłączyć usługi UAC, podczas włączania tworzenia kopii zapasowej aplikacji musisz podać poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).
  Jeśli nie chcesz wyłączyć usługi UAC, podczas włączania tworzenia kopii zapasowej aplikacji musisz podać poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).

  Uwaga
  Skorzystaj z wbudowanego konta administratora domeny, które zostało skonfigurowane w ramach operacji tworzenia domeny. Konta utworzone później nie są obsługiwane.

Wymagania dotyczące maszyn wirtualnych Hyper-V

Jeśli aplikacja działa na maszynie wirtualnej, której kopie zapasowe tworzy agent dla Hyper-V, upewnij się, że:

- System operacyjny-gość to Windows Server 2008 lub nowszy.
- W przypadku programu Hyper-V 2008 R2: system operacyjny-gość to Windows Server 2008/2008 R2/2012.
- Maszyna wirtualna nie ma żadnych dysków dynamicznych.

© Acronis International GmbH, 2003-2024

- Między hostem Hyper-V a systemem operacyjnym-gościem istnieje połączenie sieciowe. Jest ono niezbędne do wykonywania zdalnych zapytań WMI wewnątrz maszyny wirtualnej.
- Na maszynie jest wyłączona usługa kontroli konta użytkownika (UAC). Jeśli nie chcesz wyłączyć usługi UAC, podczas włączania tworzenia kopii zapasowej aplikacji musisz podać poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).
  Jeśli nie chcesz wyłączyć usługi UAC, podczas włączania tworzenia kopii zapasowej aplikacji musisz podać poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).

  Uwaga
  Skorzystaj z wbudowanego konta administratora domeny, które zostało skonfigurowane w ramach operacji tworzenia domeny. Konta utworzone później nie są obsługiwane.

- Konfiguracja maszyny wirtualnej spełnia następujące kryteria:
  - Są zainstalowane i aktualne Usługi integracji funkcji Hyper-V. Aktualizacja krytyczna to https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - W ustawieniach maszyny wirtualnej jest włączona opcja **Zarządzanie** > **Usługi integracji** > **Kopia zapasowa (punkt kontrolny woluminu)**.
  - W przypadku programu Hyper-V 2012 lub nowszego: maszyna wirtualna nie ma żadnych punktów kontrolnych.
  - W przypadku programu Hyper-V 2012 R2 lub nowszego: maszyna wirtualna ma kontroler SCSI (sprawdź **Ustawienia** > **Sprzęt**).

Kopia zapasowa bazy danych

Przed utworzeniem kopii zapasowej baz danych dopilnuj, aby zostały spełnione wymagania wymienione w sekcji „Wymagania wstępne”.

Wybierz bazy danych zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Wybieranie baz danych SQL

Kopia zapasowa bazy danych SQL zawiera pliki bazy danych (.mdf, .ndf), pliki dziennika (.ldf) i inne powiązane pliki. Kopia zapasowa tych plików jest tworzona przy użyciu usługi zapisywania programu SQL Writer. Usługa ta musi być uruchomiona, gdy Usługa kopiowania woluminów w tle (VSS) zażąda utworzenia kopii zapasowej lub odzyskania.

Po każdym pomyślnym utworzeniu kopii zapasowej są obcinane dzienniki transakcji SQL. Obcinanie dzienników SQL można wyłączyć w opcjach planu ochrony.

Aby wybrać bazy danych SQL

1. Kliknij **Urządzenia** > **Microsoft SQL**.

© Acronis International GmbH, 2003-2024

W oprogramowaniu zostanie pokazane drzewo zawsze włączonych grup dostępności (AAG) programu SQL Server, komputerów z uruchomionym programem Microsoft SQL Server, instancji programu SQL Server i baz danych.

2. Przejdź do danych, które chcesz uwzględnić w kopii zapasowej.

   Rozwiń węzły drzewa lub klikaj dwukrotnie elementy na liście po prawej stronie drzewa.
3. Wybierz dane, które chcesz uwzględnić w kopii zapasowej. Możesz wybrać zawsze włączone grupy dostępności (AAG), komputery z uruchomionym programem SQL Server, instancje programu SQL Server lub poszczególne bazy danych.
   - W przypadku wybrania zawsze włączonej grupy dostępności (AAG) w kopii zapasowej zostaną uwzględnione wszystkie bazy danych należące do wybranej zawsze włączonej grupy dostępności (AAG). Więcej informacji o tworzeniu kopii zapasowych zawsze włączonych grup dostępności lub pojedynczych baz danych zawsze włączonych grup dostępności można znaleźć w artykule „Ochrona zawsze włączonych grup dostępności”.
   - W przypadku wybrania komputera z programem SQL Server zostaną utworzone kopie zapasowe wszystkich baz danych dołączonych do wszystkich instancji SQL Server na wybranym komputerze.
   - W przypadku wybrania instancji SQL Server zostaną utworzone kopie zapasowe wszystkich baz danych przyłączonych do wybranej instancji.
   - W przypadku bezpośredniego wybrania baz danych w kopii zapasowej będą uwzględniane tylko wybrane bazy danych.
4. Kliknij **Chroń**. Jeśli pojawi się monit, podaj poświadczenia umożliwiające dostęp do danych programu SQL Server.

   W przypadku korzystania z funkcji uwierzytelniania dostępnej w systemie Windows konto musi należeć do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na danym komputerze oraz do roli **administrator systemu** w każdej instancji uwzględnianej w kopii zapasowej.

   W przypadku korzystania z funkcji uwierzytelniania dostępnej w programie SQL Server konto musi należeć do roli **administrator systemu** w każdej instancji uwzględnianej w kopii zapasowej.

Wybieranie danych programu Exchange Server

Poniższa tabela zawiera zestawienie danych programu Microsoft Exchange Server, które można wybrać do uwzględnienia w kopii zapasowej, oraz minimalne prawa użytkownika wymagane w celu utworzenia kopii zapasowej tych danych.

Wersja programu Exchange	Elementy danych	Prawa użytkownika
2007	Grupy magazynów	Członkostwo w grupie z rolą **Administratorzy organizacji korzystającej z programu Exchange**
2010/2013/2016/2019	Bazy danych, grupy dostępności bazy danych	Członkostwo w grupie z rolą **Zarządzanie serwerem**.

© Acronis International GmbH, 2003-2024

Pełna kopia zapasowa zawiera wszystkie wybrane dane programu Exchange Server.

Przyrostowa kopia zapasowa zawiera zmienione bloki plików baz danych, pliki punktów kontrolnych oraz niewielką liczbę plików dziennika nowszych niż odpowiedni punkt kontrolny bazy danych. Ponieważ w kopii zapasowej są uwzględniane zmiany wprowadzone w plikach baz danych, nie trzeba tworzyć kopii zapasowej wszystkich wpisów dzienników transakcji utworzonych od ostatniej kopii zapasowej. Tylko dziennik nowszy niż punkt kontrolny wymaga odtworzenia po odzyskaniu. Zapewnia to szybsze odzyskiwanie i pomyślne tworzenie kopii zapasowych baz danych, nawet przy włączonym rejestrowaniu cyklicznym.

Pliki dzienników transakcji są obcinane po każdym pomyślnym utworzeniu kopii zapasowej.

Aby wybrać dane programu Exchange Server

1. Kliknij **Urządzenia** > **Microsoft Exchange**.
   W oprogramowaniu zostanie pokazane drzewo grup dostępności bazy danych (DAG) programu Exchange Server, komputerów z uruchomionym programem Microsoft Exchange Server i baz danych programu Exchange Server. Jeśli agent dla programu Exchange został skonfigurowany zgodnie z opisem podanym w sekcji "Kopia zapasowa skrzynki pocztowej" (s. 612), w drzewie będą pokazywane również skrzynki pocztowe.
2. Przejdź do danych, które chcesz uwzględnić w kopii zapasowej.
   Rozwiń węzły drzewa lub klikaj dwukrotnie elementy na liście po prawej stronie drzewa.
3. Wybierz dane, które chcesz uwzględnić w kopii zapasowej.
   - W przypadku wybrania grupy DAG w kopii zapasowej znajdzie się jedna kopia każdej klastrowanej bazy danych. Dodatkowe informacje na temat tworzenia kopii zapasowych grup dostępności bazy danych (DAG) można znaleźć w sekcji "Ochrona grup dostępności bazy danych (DAG)" (s. 607).
   - W przypadku wybrania komputera z uruchomionym programem Microsoft Exchange Server w kopii zapasowej zostaną uwzględnione wszystkie bazy danych zamontowane w programie Exchange Server uruchomionym na wybranym komputerze.
   - W przypadku bezpośredniego wybrania baz danych w kopii zapasowej będą uwzględniane tylko wybrane bazy danych.
   - Jeśli agent dla programu Exchange został skonfigurowany zgodnie z opisem podanym w sekcji "Kopia zapasowa skrzynki pocztowej" (s. 612), można wybrać skrzynki pocztowe do uwzględnienia w kopii zapasowej.

   Jeśli wybór obejmuje wiele baz danych, są one przetwarzane po dwie naraz. Gdy zakończy się operacja tworzenia kopii zapasowej pierwszej grupy, rozpocznie się tworzenie kopii zapasowej drugiej grupy itd.
4. Jeśli pojawi się monit, podaj poświadczenia umożliwiające dostęp do danych.
5. Kliknij **Chroń**.

© Acronis International GmbH, 2003-2024

Ochrona zawsze włączonych grup dostępności (AAG)

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Przegląd rozwiązań dla SQL Server o wysokiej dostępności

Funkcja Windows Server Failover Clustering (WSFC) umożliwia skonfigurowanie SQL Server o wysokiej dostępności przez zastosowanie nadmiarowości na poziomie instancji (Failover Cluster Instance, FCI) lub na poziomie bazy danych (AlwaysOn Availability Group, AAG). Można również łączyć obie te metody.

W metodzie Failover Cluster Instance bazy danych SQL znajdują się w magazynie współużytkowanym. Do tego magazynu można uzyskać dostęp wyłącznie z aktywnego węzła klastra. W przypadku awarii aktywnego węzła następuje przełączenie awaryjne i aktywny staje się inny węzeł.

W grupie dostępności każda replika bazy danych znajduje się w innym węźle. Jeśli replika główna staje się niedostępna, jej rola jest przypisywana replice dodatkowej znajdującej się w innym węźle.

Dlatego też już same klastry stanowią rozwiązanie odzyskiwania po awarii. Mogą jednak wystąpić sytuacje, kiedy klastry nie mogą zapewnić ochrony danych: na przykład w przypadku logicznego uszkodzenia bazy danych lub uszkodzenia całego klastra. Ponadto rozwiązania klastrowe nie chronią przed szkodliwymi zmianami zawartości, ponieważ zwykle natychmiast replikują dane do wszystkich węzłów klastra.

Obsługiwane konfiguracje klastrów

To oprogramowanie do tworzenia kopii zapasowych obsługuje *wyłącznie* zawsze włączoną grupę dostępności (AAG) w przypadku programu SQL Server 2012 lub nowszego. Inne konfiguracje klastrów, np. instancje klastrów awaryjnych, dublowanie bazy danych i wysyłanie dziennika *nie* są obsługiwane.

Ile agentów jest wymaganych do tworzenia kopii zapasowej i odzyskiwania danych klastra?

Aby pomyślnie utworzyć kopię zapasową danych agenta dla języka SQL i odzyskać ją, w każdym węźle klastra WSFC musi być zainstalowany agent dla języka SQL.

Tworzenie kopii zapasowych baz danych uwzględnionych w grupie AAG

1. Zainstaluj agenta dla języka SQL we wszystkich węzłach klastra WSFC.
2. Wybierz grupę AAG do utworzenia kopii zapasowej zgodnie z opisem w sekcji Wybieranie „Wybieranie baz danych SQL”.

© Acronis International GmbH, 2003-2024

Musisz wybrać samą grupę AAG, aby utworzyć kopię zapasową wszystkich jej baz danych. Aby utworzyć kopię zapasową zestawu baz danych, zdefiniuj ten zestaw na wszystkich węzłach grupy AAG.

Ostrzeżenie!
Zestaw baz danych musi być dokładnie taki sam na wszystkich węzłach. Jeśli choć jeden zestaw będzie inny lub zestaw nie zostanie zdefiniowany na wszystkich węzłach, operacja tworzenia kopii zapasowej klastra nie przebiegnie poprawnie.

3. Skonfiguruj opcję kopii zapasowej „Tryb tworzenia kopii zapasowych klastra".

Odzyskiwanie baz danych uwzględnionych w grupie AAG

1. Wybierz bazy danych, które chcesz odzyskać, a następnie wybierz punkt odzyskiwania, z którego chcesz odzyskać bazy danych.

   Jeśli wybierzesz klastrowaną bazę danych w pozycji **Urządzenia** > **Microsoft SQL** > **Bazy danych**, a następnie klikniesz opcję **Odzyskaj**, oprogramowanie wyświetli tylko punkty odzyskiwania związane z czasami, w których utworzono kopię zapasową wybranej kopii bazy danych.

   Najłatwiejszym sposobem na wyświetlenie wszystkich punktów odzyskiwania klastrowanej bazy danych jest wybranie kopii zapasowej całej grupy AAG na karcie Magazyn kopii zapasowych.Kopie zapasowe grupy AAG mają nazwy zgodne z następującym szablonem: `<nazwa grupy AAG> - <nazwa planu ochrony>` i są oznaczane specjalną ikoną.
2. Aby skonfigurować odzyskiwanie, wykonaj kroki opisane w części „Odzyskiwanie baz danych SQL", rozpoczynając od kroku 5.

   Oprogramowanie automatycznie zdefiniuje węzeł klastra, do którego zostaną odzyskane dane. Nazwa węzła jest wyświetlana w polu **Odzyskaj do**. Możesz ręcznie zmienić węzeł docelowy.

Ważne
Bazy danych dołączonej do zawsze włączonej grupy dostępności nie można zastąpić podczas odzyskiwania, ponieważ uniemożliwia to program Microsoft SQL Server. Przed rozpoczęciem odzyskiwania należy wykluczyć docelową bazę danych z grupy AAG. Można również odzyskać bazę danych jako nową bazę nie należącą do grupy AAG. Po zakończeniu odzyskiwania można przywrócić oryginalną konfigurację grupy AAG.

Ochrona grup dostępności bazy danych (DAG)

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Przegląd klastrów programu Exchange Server

Podstawowym celem stosowania klastrów programu Exchange jest zapewnienie wysokiej dostępności bazy danych, szybkie przełączanie awaryjne i ochrona przed utratą danych. Zwykle

© Acronis International GmbH, 2003-2024

osiąga się go przez utworzenie co najmniej jednej kopii baz danych lub grup magazynów w członkach (węzłach) klastra. Jeśli dojdzie do awarii węzła klastra, w którym znajduje się aktywna kopia bazy danych, lub awarii samej aktywnej kopii bazy danych, drugi węzeł, w którym znajduje się pasywna kopia, automatycznie przejmie operacje uszkodzonego węzła i zapewni dostęp do usług programu Exchange z minimalnym czasem przestoju. Dlatego też już same klastry stanowią rozwiązanie odzyskiwania po awarii.

Mogą jednak wystąpić sytuacje, kiedy klastrowe rozwiązania przełączania awaryjnego nie mogą zapewnić ochrony danych, na przykład w przypadku logicznego uszkodzenia bazy danych, braku kopii (repliki) określonej bazy danych w klastrze lub uszkodzenia całego klastra. Ponadto rozwiązania klastrowe nie chronią przed szkodliwymi zmianami zawartości, ponieważ zwykle natychmiast replikują dane do wszystkich węzłów klastra.

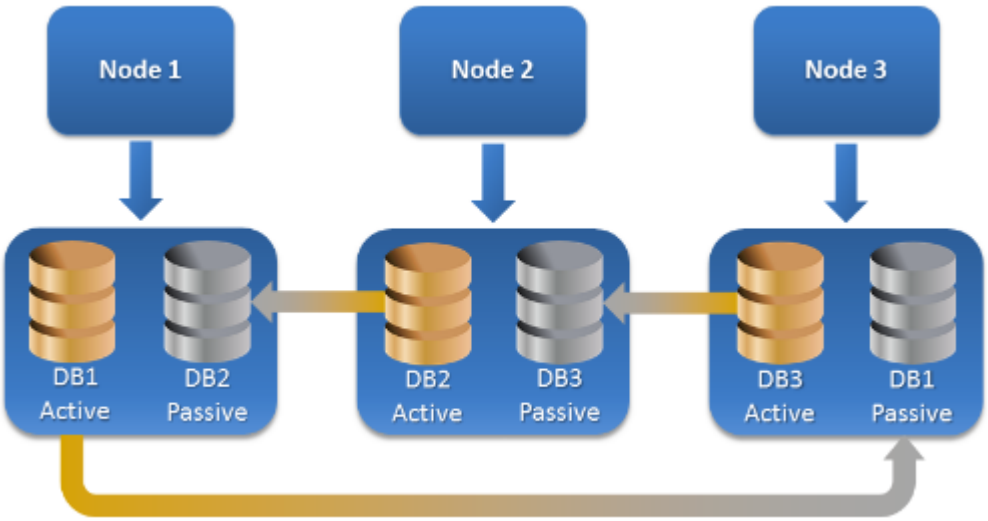
Kopia zapasowa uwzględniająca klastry

W przypadku kopii zapasowej uwzględniającej klastry w kopii zapasowej jest umieszczany tylko jeden egzemplarz danych z klastrów. Jeśli dane zapisywane w kopii zapasowej zmienią swoją lokalizację w klastrze (na przykład w wyniku przełączenia lub przełączenia awaryjnego), program będzie monitorować wszystkie przeniesienia tych danych i bezpiecznie utworzy ich kopię zapasową.

Obsługiwane konfiguracje klastrów

Kopia zapasowa uwzględniająca klastry jest obsługiwana *tylko* w przypadku grupy dostępności bazy danych w programie Exchange Server 2010 lub nowszym. Inne konfiguracje klastrów, np. klastry pojedynczej kopii oraz ciągła replikacja klastra dla programu Exchange 2007, *nie* są obsługiwane.

DAG to grupa maksymalnie 16 serwerów skrzynek pocztowych programu Exchange. Każdy z węzłów może przechowywać kopię bazy danych skrzynki pocztowej z dowolnego z pozostałych węzłów. Każdy z węzłów może przechowywać pasywne i aktywne kopie bazy danych. Możliwe jest utworzenie nawet 16 kopii każdej z baz danych.



© Acronis International GmbH, 2003-2024

Ile agentów potrzeba do utworzenia kopii zapasowej uwzględniającej klastry i odzyskania z niej danych?

Aby pomyślnie utworzyć kopię zapasową klastrowanych baz danych i odzyskać je, w każdym węźle klastra programu Exchange musi być zainstalowany agent dla programu Exchange.

Uwaga
Po zainstalowaniu agenta na jednym z węzłów w konsoli Cyber Protect zostanie wyświetlona grupa dostępności baz danych i jej węzły w obszarze **Urządzenia** > **Microsoft Exchange** > **Bazy danych**. Aby zainstalować agenty dla programu Exchange w pozostałych węzłach, wybierz grupę DAG, kliknij pozycję **Szczegóły**, a następnie kliknij opcję **Zainstaluj agenta** obok każdego z węzłów.

Tworzenie kopii zapasowej danych klastra programu Exchange

1. Podczas tworzenia planu ochrony wybierz grupę dostępności baz danych zgodnie z opisem podanym w sekcji "Wybieranie danych programu Exchange Server" (s. 604).
2. Skonfiguruj opcję kopii zapasowej "Tryb tworzenia kopii zapasowych klastra" (s. 490).
3. Odpowiednio określ inne ustawienia planu ochrony.

Ważne
W przypadku tworzenia kopii zapasowej uwzględniającej klastry koniecznie wybierz całą grupę dostępności baz danych. Jeśli wybierzesz poszczególne węzły lub bazy danych w tej grupie, w kopii zapasowej zostaną uwzględnione tylko wybrane elementy, a opcja **Tryb tworzenia kopii zapasowych klastra** zostanie zignorowana.

Odzyskiwanie danych klastra programu Exchange

1. Wybierz punkt odzyskiwania dla bazy danych, którą chcesz odzyskać. Nie można wybrać odzyskania całego klastra.

   Jeśli w pozycji **Urządzenia** > **Microsoft Exchange** > **Bazy danych** > `<nazwa klastra>` > `<nazwa węzła>` wybierzesz kopię klastrowanej bazy danych, a następnie klikniesz **Odzyskaj**, oprogramowanie wyświetli tylko punkty odzyskiwania związane z czasami, w których utworzono kopię zapasową wybranej bazy.

   Najłatwiejszym sposobem na wyświetlenie wszystkich punktów odzyskiwania klastrowanej bazy danych jest wybranie jej kopii zapasowej na karcie Magazyn kopii zapasowych.
2. Wykonaj czynności opisane w sekcji "Odzyskiwanie baz danych programu Exchange" (s. 623), zaczynając od kroku 5.

   Oprogramowanie automatycznie zdefiniuje węzeł klastra, do którego zostaną odzyskane dane. Nazwa węzła jest wyświetlana w polu **Odzyskaj do**. Możesz ręcznie zmienić węzeł docelowy.

Kopia zapasowa uwzględniająca aplikacje

Uwzględniająca aplikacje kopia zapasowa na poziomie dysku jest dostępna w przypadku komputerów fizycznych, maszyn wirtualnych ESXi i maszyn wirtualnych Hyper-V.

© Acronis International GmbH, 2003-2024

W przypadku tworzenia kopii zapasowej komputera z programem Microsoft SQL Server, programem Microsoft Exchange Server lub usługami domenowymi Active Directory włącz **Kopia zapasowa aplikacji**, aby zyskać dodatkową ochronę danych tych aplikacji.

Dlaczego warto korzystać z kopii zapasowej uwzględniającej aplikacje?

Używanie kopii zapasowej uwzględniającej aplikacje przynosi następujące korzyści:

- Aplikacje są uwzględniane w kopii zapasowej w spójnym stanie, dzięki czemu będą dostępne natychmiast po odzyskaniu maszyny.
- Bazy danych SQL oraz bazy danych, skrzynki pocztowe i elementy skrzynek pocztowych programu Exchange można odzyskać bez odzyskiwania całej maszyny.
- Po każdym pomyślnym utworzeniu kopii zapasowej są obcinane dzienniki transakcji SQL. Obcinanie dzienników SQL można wyłączyć w opcjach planu ochrony. Dzienniki transakcji programu Exchange są obcinane tylko na maszynach wirtualnych. Jeśli dzienniki transakcji programu Exchange mają być obcinane na komputerze fizycznym, włącz opcję Pełne kopie zapasowe z usługą VSS.
- Jeśli domena zawiera więcej niż jeden kontroler domeny i jeden z nich zostanie odzyskany, wykonywane jest przywracanie nieautorytatywne i po odzyskaniu nie nastąpi wycofanie numeru USN.

Co jest potrzebne do skorzystania z kopii zapasowej uwzględniającej aplikacje?

Na komputerze fizycznym oprócz agenta dla systemu Windows musi być zainstalowany agent dla SQL i/lub agent dla programu Exchange.

W przypadku maszyny wirtualnej nie jest wymagana instalacja żadnego agenta — zakłada się, że kopia zapasowa maszyny jest tworzona przez agenta dla VMware (w systemie Windows) lub agenta dla Hyper-V.

Uwaga
W przypadku maszyn wirtualnych Hyper-V i VMware ESXi z systemem Windows Server 2022 tworzenie kopii zapasowych uwzględniających aplikacje nie jest obsługiwane w trybie bezagentowym, czyli kiedy kopia zapasowa jest tworzona odpowiednio przez agenta dla Hyper-V lub agenta dla VMware. Aby chronić aplikacje firmy Microsoft na tych maszynach, trzeba zainstalować agenta dla systemu Windows w systemie operacyjnym gościa.

Agent dla VMware (urządzenie wirtualne) może tworzyć kopie zapasowe uwzględniające aplikacje, ale nie może odzyskiwać danych aplikacji z tych kopii. Aby odzyskać dane aplikacji z kopii zapasowych utworzonych przez tego agenta, potrzebny jest agent dla VMware (Windows), agent dla

© Acronis International GmbH, 2003-2024

SQL lub agent dla programu Exchange zainstalowany na komputerze, który ma dostęp do lokalizacji przechowywania tych kopii zapasowych. Konfigurując odzyskiwanie danych aplikacji, wybierz punkt odzyskiwania na karcie **Magazyn kopii zapasowych**, a następnie wybierz dany komputer w polu **Komputer używany do przeglądania**.

Inne wymagania podano w sekcjach „Wymagania wstępne” i „Wymagane prawa użytkownika”.

Uwaga
Operacje tworzenia kopii zapasowych maszyn wirtualnych Hyper-V z uwzględnieniem aplikacji mogą się kończyć niepowodzeniem z błędem „Nie można wykonać zapytania WMI »ExecQuery«” lub „Nie można utworzyć nowego procesu za pośrednictwem WMI”, jeśli kopie zapasowe są tworzone na hoście przy dużym obciążeniu, z powodu braku lub opóźnionej odpowiedzi z usługi Instrumentacja zarządzania Windows. Operacje tworzenia kopii zapasowych mogą być ponawiane w przedziale czasowym, w którym obciążenie hosta jest mniejsze.

Wymagane prawa użytkownika w przypadku tworzenia kopii zapasowych uwzględniających aplikacje

Kopia zapasowa uwzględniająca aplikacje zawiera metadane znajdujących się na dysku aplikacji uwzględniających usługę VSS. Aby uzyskać dostęp do tych metadanych, agent potrzebuje konta z odpowiednimi prawami. Wymieniono je poniżej. Podczas włączania tworzenia kopii zapasowej aplikacji pojawi się monit o określenie tego konta.

- W przypadku programu SQL Server:
  Konto musi należeć do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na komputerze i być członkiem roli **sysadmin** w każdej instancji, w której przypadku chcesz utworzyć kopię zapasową.

  Uwaga
  Obsługiwane jest tylko uwierzytelnianie systemu Windows.

- W przypadku programu Exchange Server:
  Exchange 2007: Konto musi należeć do grupy **Administratorzy** na komputerze i do grupy z rolą **Administratorzy organizacji korzystającej z programu Exchange**.
  Program Exchange 2010 lub nowszy: Konto musi należeć do grupy **Administratorzy** na komputerze i do grupy z rolą **Zarządzanie organizacją**.
- W przypadku usługi Active Directory:
  Konto musi być administratorem domeny.

Dodatkowe wymaganie dotyczące maszyn wirtualnych

Jeśli aplikacja działa na maszynie wirtualnej, której kopie zapasowe tworzy agent dla VMware lub agent dla Hyper-V, upewnij się, że na tej maszynie jest wyłączona usługa kontroli konta użytkownika.

Jeśli nie chcesz wyłączyć usługi UAC, podczas włączania tworzenia kopii zapasowej aplikacji musisz podać poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).

© Acronis International GmbH, 2003-2024

Uwaga
Skorzystaj z wbudowanego konta administratora domeny, które zostało skonfigurowane w ramach operacji tworzenia domeny. Konta utworzone później nie są obsługiwane.

Dodatkowe wymagania w przypadku komputerów z systemami operacyjnymi Windows

W każdej wersji systemu Windows trzeba wyłączyć zasady kontroli konta użytkownika, aby można było tworzyć kopie zapasowe uwzględniające aplikacje.

Jeśli nie chcesz wyłączyć usługi UAC, podczas włączania tworzenia kopii zapasowej aplikacji musisz podać poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).

Uwaga
Skorzystaj z wbudowanego konta administratora domeny, które zostało skonfigurowane w ramach operacji tworzenia domeny. Konta utworzone później nie są obsługiwane.

Aby wyłączyć zasady kontroli konta użytkownika w systemie Windows

1. W Edytorze rejestru odszukaj następujący klucz rejestru:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Zmień wartość klucza **EnableLUA** na **0**.
3. Uruchom ponownie komputer.

Kopia zapasowa skrzynki pocztowej

Kopia zapasowa skrzynki pocztowej jest obsługiwana w przypadku programu Microsoft Exchange Server 2010 z dodatkiem Service Pack 1 (SP1) lub nowszego.

Kopia zapasowa skrzynki pocztowej jest dostępna, jeśli na serwerze zarządzania jest zarejestrowany przynajmniej jeden agent dla programu Exchange. Agent musi być zainstalowany na komputerze należącym do tego samego lasu usługi Active Directory co program Microsoft Exchange Server.

Przed utworzeniem kopii zapasowej skrzynek pocztowych musisz połączyć agenta dla programu Exchange z komputerem z rolą serwera **Dostęp klienta** (CAS) programu Microsoft Exchange Server. W programie Exchange 2016 lub jego nowszej wersji rola CAS nie jest dostępna jako osobna opcja instalacji. Jest automatycznie instalowana w ramach roli serwera Skrzynka pocztowa. W związku z tym można połączyć agenta z dowolnym serwerem z **rolą Skrzynka pocztowa**.

Uwaga
Skrzynki pocztowe i elementy skrzynek pocztowych można odzyskiwać z kopii zapasowych baz danych i kopii zapasowych uwzględniających aplikacje. Aby uzyskać więcej informacji, zobacz "Odzyskiwanie skrzynek pocztowych programu Exchange i ich elementów" (s. 626). W przypadku kopii zapasowych baz danych i kopii zapasowych uwzględniających aplikacje nie można tworzyć planów ochrony dla pojedynczych skrzynek pocztowych.

Aby połączyć agenta dla programu Exchange z CAS

© Acronis International GmbH, 2003-2024

1. Kliknij **Urządzenia** > **Dodaj**.
2. Kliknij opcję **Microsoft Exchange Server**.
3. Kliknij **Skrzynki pocztowe programu Exchange**.

   Jeśli na serwerze zarządzania nie zarejestrowano żadnego agenta dla programu Exchange, oprogramowanie zasugeruje zainstalowanie tego agenta. Po zakończeniu instalacji powtórz procedurę, zaczynając od kroku 1.
4. [Opcjonalnie] Jeśli na serwerze zarządzania zarejestrowano kilka agentów dla programu Exchange, kliknij **Agent**, a następnie zmień agenta, które utworzy kopię zapasową.
5. W sekcji **Serwer dostępu klienta** określ w pełni kwalifikowaną nazwę domeny (FQDN) komputera z rolą **Dostęp klienta** programu Microsoft Exchange Server.

   W programie Exchange 2016 lub jego nowszej wersji usługi dostępu klienta są automatycznie instalowane w ramach roli serwera Skrzynka pocztowa. W związku z tym można określić dowolny serwer z **rolą Skrzynka pocztowa**. W dalszej części tej sekcji ten serwer jest określany jako serwer CAS.
6. W sekcji **Typ uwierzytelniania** wybierz typ uwierzytelniania, który jest używany przez serwer CAS. Możesz wybrać typ **Kerberos** (domyślny) lub **Podstawowe**.
7. [Tylko w przypadku uwierzytelniania podstawowego] Wybierz protokół, który będzie używany. Możesz wybrać protokół **HTTPS** (domyślny) lub **HTTP**.
8. [Tylko w przypadku uwierzytelniania podstawowego przy użyciu protokołu HTTPS] Jeśli serwer CAS korzysta z certyfikatu SSL uzyskanego od podmiotu certyfikującego i chcesz, aby oprogramowanie sprawdzało ten certyfikat podczas nawiązywania połączenia z serwerem CAS, zaznacz pole wyboru **Sprawdź certyfikat SSL**. W przeciwnym razie pomiń ten krok.
9. Określ poświadczenia konta, które będzie używane w celu uzyskania dostępu do serwera CAS. Wymagania wobec takiego konta znajdują się w sekcji „Wymagane prawa użytkownika”.
10. Kliknij **Dodaj**.

Wskutek tego skrzynki pocztowe pojawią się w pozycji **Urządzenia** > **Microsoft Exchange** > **Skrzynki pocztowe**.

Wybieranie skrzynek pocztowych programu Exchange Server

Wybierz skrzynki pocztowe zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać skrzynki pocztowe programu Exchange

1. Kliknij **Urządzenia** > **Microsoft Exchange**.

   Program wyświetli drzewo baz danych programu Exchange i skrzynek pocztowych.
2. Kliknij **Skrzynki pocztowe**, a następnie wybierz skrzynki pocztowe, które chcesz uwzględnić w kopii zapasowej.
3. Kliknij **Chroń**.

© Acronis International GmbH, 2003-2024

Wymagane prawa użytkownika

Aby uzyskać dostęp do skrzynek pocztowych, agent do programu Exchange potrzebuje konta z odpowiednimi uprawnieniami. Podczas konfigurowania różnych operacji na skrzynkach pocztowych pojawi się monit o określenie tego konta.

Przynależność konta do grupy z rolą **zarządzania organizacją** pozwala uzyskać dostęp do każdej skrzynki pocztowej, również do skrzynek tworzonych w przyszłości.

Minimalne wymagane prawa użytkownika:

- Konto musi należeć do grup ról **Zarządzanie serwerem** i **Zarządzanie odbiorcami**.
- Konto musi mieć rolę **ApplicationImpersonation** i musi być ona włączona dla wszystkich użytkowników lub grup użytkowników, do których skrzynek pocztowych agent będzie mieć dostęp.

  Aby uzyskać informacje na temat konfiguracji roli zarządzania **ApplicationImpersonation**, przeczytaj następujący artykuł bazy wiedzy firmy Microsoft: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

Odzyskiwanie baz danych SQL

Bazy danych SQL można odzyskiwać z kopii zapasowych baz danych i kopii zapasowych uwzględniających aplikacje. Dodatkowe informacje o różnicach między tymi dwoma typami kopii zapasowych można znaleźć w sekcji "Chronienie programów Microsoft SQL Server i Microsoft Exchange Server" (s. 599).

Bazy danych SQL można odzyskać do ich pierwotnej instancji, do innej instancji na pierwotnym komputerze lub do instancji na komputerze innym niż pierwotny. W przypadku odzyskiwania na komputer inny niż pierwotny na tym komputerze docelowym musi być zainstalowany agent dla SQL.

Bazy danych można też odzyskiwać w formie plików.

W przypadku używania funkcji uwierzytelniania dostępnej w systemie Windows na potrzeby instancji SQL trzeba podać poświadczenia konta należącego do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na danym komputerze oraz do roli **administratora systemu** w instancji docelowej. W przypadku korzystania z funkcji uwierzytelniania dostępnej w programie SQL Server trzeba podać poświadczenia konta należącego do roli **administratora systemu** w instancji docelowej.

Systemowe bazy danych są odzyskiwane jako bazy danych użytkowników, z pewnymi różnicami. Dodatkowe informacje na temat tych różnic można znaleźć w sekcji "Odzyskiwanie systemowych baz danych" (s. 621).

Podczas odzyskiwania można sprawdzać postęp operacji w konsoli Cyber Protect, na karcie **Monitorowanie** > **Działania**.

© Acronis International GmbH, 2003-2024

Odzyskiwanie baz danych SQL na pierwotny komputer

Bazy danych SQL można odzyskać do ich pierwotnej instancji, do innej instancji na pierwotnym komputerze lub do instancji na komputerze docelowym innym niż pierwotny.

Aby odzyskać bazy danych SQL na pierwotny komputer

Z kopii zapasowej baz danych

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft SQL**.
2. Wybierz instancję SQL Server lub kliknij nazwę instancji, aby wybrać bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Aby odzyskać dane na inny komputer niż pierwotny, zobacz sekcję "Odzyskiwanie baz danych SQL na komputer inny niż pierwotny" (s. 617).
3. Wybierz punkt odzyskiwania.

   Punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Bazy danych do instancji**.

   Domyślnie instancja i bazy danych są odzyskiwane do pierwotnych lokalizacji. Można też odzyskać oryginalną bazę danych jako nową bazę danych.
5. [W przypadku odzyskiwania do innej instancji niż pierwotna na tym samym komputerze] Kliknij **Docelowa instancja SQL Server**, wybierz instancję docelową, a następnie kliknij **Gotowe**.
6. [W przypadku odzyskiwania bazy danych jako nowej bazy danych] Kliknij nazwę bazy danych, a następnie w polu **Odzyskaj do** wybierz **Nowa baza danych**.
   - Określ nazwę nowej bazy danych.
   - Podaj ścieżkę nowej bazy danych.
   - Podaj ścieżkę dziennika.
7. [Opcjonalnie] [Działanie niedostępne w przypadku odzyskiwania bazy danych jako nowej bazy danych] Aby zmienić stan bazy danych po odzyskaniu, kliknij jej nazwę i wybierz jeden z poniższych stanów, a następnie kliknij **Gotowe**.
   - **Gotowe do użycia (PRZYWRACANIE Z ODZYSKIWANIEM)** (domyślny)

     Po zakończeniu odzyskiwania baza danych będzie gotowa do użycia. Użytkownicy będą mieli do niej pełny dostęp. Program cofnie wszystkie niezatwierdzone transakcje odzyskanej bazy danych zapisane w dziennikach transakcji. Odzyskanie dodatkowych dzienników transakcji z macierzystych kopii zapasowych programu Microsoft SQL będzie niemożliwe.
   - **Niegotowe do użycia (PRZYWRACANIE BEZ ODZYSKIWANIA)**

     Po zakończeniu odzyskiwania baza danych nie będzie gotowa do użycia. Użytkownicy nie będą mieli do niej dostępu. Program zachowa wszystkie niezatwierdzone transakcje odzyskanej bazy danych. Będzie możliwe odzyskanie dodatkowych dzienników transakcji z macierzystych kopii zapasowych programu Microsoft SQL, a tym samym osiągnięcie odpowiedniego punktu odzyskiwania.
   - **Tylko do odczytu (PRZYWRACANIE W STANIE GOTOWOŚCI)**

© Acronis International GmbH, 2003-2024

Po zakończeniu odzyskiwania użytkownicy będą mieli dostęp tylko do odczytu do bazy danych. Program cofnie wszystkie niezatwierdzone transakcje. Zapisze jednak czynności cofania w tymczasowym pliku rezerwowym, aby było możliwe przywrócenie stanu sprzed odzyskania.

Ta wartość jest używana głównie w celu wykrycia punktu w czasie, w którym wystąpił błąd programu SQL Server.

8. Kliknij **Rozpocznij odzyskiwanie**.

Z kopii zapasowej uwzględniającej aplikacje

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputer, który pierwotnie zawierał dane do odzyskania, a następnie kliknij **Odzyskiwanie**.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Aby odzyskać dane na inny komputer niż pierwotny, zobacz sekcję "Odzyskiwanie baz danych SQL na komputer inny niż pierwotny" (s. 617).
3. Wybierz punkt odzyskiwania.

   Punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Bazy danych SQL**.
5. Wybierz instancję serwera SQL lub kliknij nazwę instancji, aby wybrać bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.

   Domyślnie instancja i bazy danych są odzyskiwane do pierwotnych lokalizacji. Można też odzyskać oryginalną bazę danych jako nową bazę danych.
6. [W przypadku odzyskiwania do innej instancji niż pierwotna na tym samym komputerze] Kliknij **Docelowa instancja SQL Server**, wybierz instancję docelową, a następnie kliknij **Gotowe**.
7. [W przypadku odzyskiwania bazy danych jako nowej bazy danych] Kliknij nazwę bazy danych, a następnie w polu **Odzyskaj do** wybierz **Nowa baza danych**.
   - Określ nazwę nowej bazy danych.
   - Podaj ścieżkę nowej bazy danych.
   - Podaj ścieżkę dziennika.
8. [Opcjonalnie] [Działanie niedostępne w przypadku odzyskiwania bazy danych jako nowej bazy danych] Aby zmienić stan bazy danych po odzyskaniu, kliknij jej nazwę i wybierz jeden z poniższych stanów, a następnie kliknij **Gotowe**.
   - **Gotowe do użycia (PRZYWRACANIE Z ODZYSKIWANIEM)** (domyślny)

     Po zakończeniu odzyskiwania baza danych będzie gotowa do użycia. Użytkownicy będą mieli do niej pełny dostęp. Program cofnie wszystkie niezatwierdzone transakcje odzyskanej bazy danych zapisane w dziennikach transakcji. Odzyskanie dodatkowych dzienników transakcji z macierzystych kopii zapasowych programu Microsoft SQL będzie niemożliwe.
   - **Niegotowe do użycia (PRZYWRACANIE BEZ ODZYSKIWANIA)**

     Po zakończeniu odzyskiwania baza danych nie będzie gotowa do użycia. Użytkownicy nie będą mieli do niej dostępu. Program zachowa wszystkie niezatwierdzone transakcje odzyskanej bazy danych. Będzie możliwe odzyskanie dodatkowych dzienników transakcji z macierzystych

 © Acronis International GmbH, 2003-2024

kopii zapasowych programu Microsoft SQL, a tym samym osiągnięcie odpowiedniego punktu odzyskiwania.

- **Tylko do odczytu (PRZYWRACANIE W STANIE GOTOWOŚCI)**

  Po zakończeniu odzyskiwania użytkownicy będą mieli dostęp tylko do odczytu do bazy danych. Program cofnie wszystkie niezatwierdzone transakcje. Zapisze jednak czynności cofania w tymczasowym pliku rezerwowym, aby było możliwe przywrócenie stanu sprzed odzyskania.

  Ta wartość jest używana głównie w celu wykrycia punktu w czasie, w którym wystąpił błąd programu SQL Server.

9. Kliknij **Rozpocznij odzyskiwanie**.

Odzyskiwanie baz danych SQL na komputer inny niż pierwotny

Zarówno kopie zapasowe uwzględniające aplikacje, jak i kopie zapasowe baz danych można odzyskać do instancji SQL Server zainstalowanej na innym niż pierwotny komputerze docelowym, na którym jest zainstalowany agent dla SQL. Kopie zapasowe muszą się znajdować w chmurze lub magazynie współużytkowanym, do których ma dostęp komputer docelowy.

Wersja programu SQL Server na komputerze docelowym musi być taka sama jak wersja na komputerze źródłowym lub nowsza.

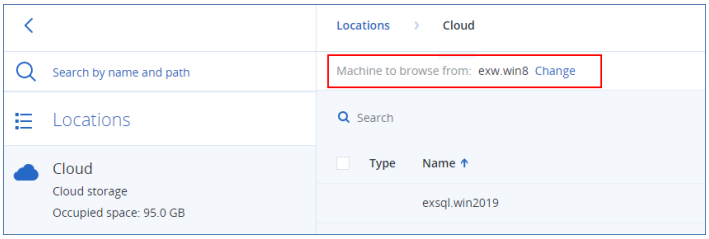
Aby odzyskać bazy danych SQL na komputer inny niż pierwotny

Z magazynu kopii zapasowych

Ta procedura dotyczy kopii zapasowych uwzględniających aplikacje i kopii zapasowych baz danych.

1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych**.
2. Wybierz lokalizację zestawu kopii zapasowych, z którego chcesz odzyskać dane.
3. W polu **Komputer używany do przeglądania** wybierz komputer docelowy.

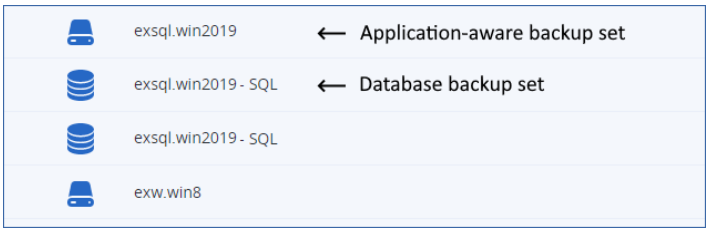
   Jest to komputer, na który zostaną odzyskane dane. Komputer docelowy musi być w trybie online.



4. Wybierz zestaw kopii zapasowych, a następnie w panelu **Czynności** kliknij **Pokaż kopie zapasowe**.

   Ikony zestawów kopii zapasowych uwzględniających aplikacje i zestawów kopii zapasowych baz danych różnią się od siebie.

© Acronis International GmbH, 2003-2024



5. Wybierz punkt odzyskiwania, z którego chcesz odzyskać dane.
6. [W przypadku kopii zapasowych baz danych] Kliknij **Odzyskaj bazy danych SQL**.
7. [W przypadku kopii zapasowych uwzględniających aplikacje] Kliknij **Odzyskaj** > **Bazy danych SQL**.
8. Wybierz instancję SQL Server lub kliknij nazwę instancji, aby wybrać bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
9. [Jeśli na komputerze docelowym jest więcej niż jedna instancja SQL] Kliknij **Docelowa instancja SQL Server**, wybierz instancję docelową, a następnie kliknij **Gotowe**.
10. Kliknij nazwę bazy danych, podaj ścieżkę nowej bazy danych i ścieżkę dziennika, a następnie kliknij **Gotowe**.

    W obu polach możesz podać tę samą ścieżkę, na przykład:

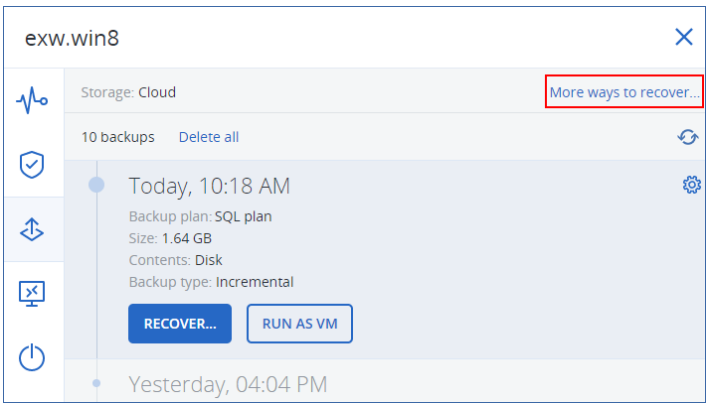
    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```

11. Kliknij **Rozpocznij odzyskiwanie**.

Z urządzeń

Ta procedura dotyczy kopii zapasowych uwzględniających aplikacje.

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputer, który pierwotnie zawierał dane do odzyskania, a następnie kliknij **Odzyskiwanie**.
3. [Jeśli komputer źródłowy jest w trybie online] Kliknij **Więcej metod odzyskiwania**.



4. Kliknij **Wybierz komputer**, aby wybrać komputer docelowy, a następnie kliknij **OK**.

   Jest to komputer, na który zostaną odzyskane dane. Komputer docelowy musi być w trybie online.
5. Wybierz punkt odzyskiwania.

© Acronis International GmbH, 2003-2024

Punkty odzyskiwania są filtrowane na podstawie lokalizacji.

6. Kliknij **Odzyskaj** > **Bazy danych SQL**.
7. Wybierz instancję SQL Server lub kliknij nazwę instancji, aby wybrać bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
8. [Jeśli na komputerze docelowym jest więcej niż jedna instancja SQL] Kliknij **Docelowa instancja SQL Server**, wybierz instancję docelową, a następnie kliknij **Gotowe**.
9. Kliknij nazwę bazy danych, podaj ścieżkę nowej bazy danych i ścieżkę dziennika, a następnie kliknij **Gotowe**.

   W obu polach możesz podać tę samą ścieżkę, na przykład:

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```

10. Kliknij **Rozpocznij odzyskiwanie**.

Odzyskiwanie baz danych SQL jako plików

Bazy danych można odzyskiwać w formie plików. Ta opcja może być przydatna, jeśli trzeba wyodrębnić dane na potrzeby wydobywania danych, inspekcji lub dalszego przetwarzania za pomocą narzędzi innych firm. Instrukcje dołączania plików baz danych SQL do instancji SQL Server można znaleźć w sekcji "Dołączanie baz danych programu SQL Server" (s. 622).

Bazy danych można odzyskać jako pliki na pierwotny komputer lub na inne komputery docelowe, na których jest zainstalowany agent dla SQL. W przypadku odzyskiwania danych na komputery inne niż pierwotny kopie zapasowe muszą się znajdować w chmurze lub magazynie współużytkowanym, do których ma dostęp komputer docelowy.

Uwaga
Odzyskiwanie baz danych jako plików jest jedyną metodą odzyskiwania dostępną w przypadku korzystania z agenta dla VMware (Windows). Nie można odzyskiwać baz danych za pomocą agenta dla VMware (urządzenie wirtualne).

Aby odzyskać bazy danych SQL jako pliki

Z kopii zapasowej baz danych

Procedura ta dotyczy komputerów źródłowych w trybie online.

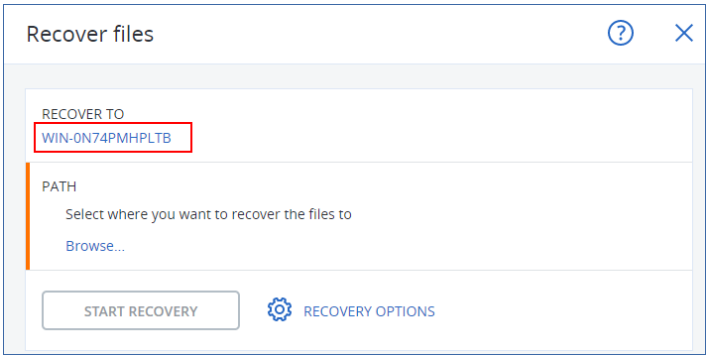
1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft SQL**.
2. Wybierz bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania.

   Punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Bazy danych jako pliki**.
5. [W przypadku odzyskiwania na inny komputer niż pierwotny] W polu **Odzyskaj do** wybierz komputer docelowy.

© Acronis International GmbH, 2003-2024

Jest to komputer, na który zostaną odzyskane dane. Komputer docelowy musi być w trybie online.

Aby zmienić wybór, kliknij nazwę komputera, wybierz inny komputer, a następnie kliknij **OK**.



6. W polu **Ścieżka** kliknij **Przeglądaj**, wybierz folder lokalny lub sieciowy, w którym mają zostać zapisane pliki, a następnie kliknij **Gotowe**.
7. Kliknij **Rozpocznij odzyskiwanie**.

Z kopii zapasowej uwzględniającej aplikacje

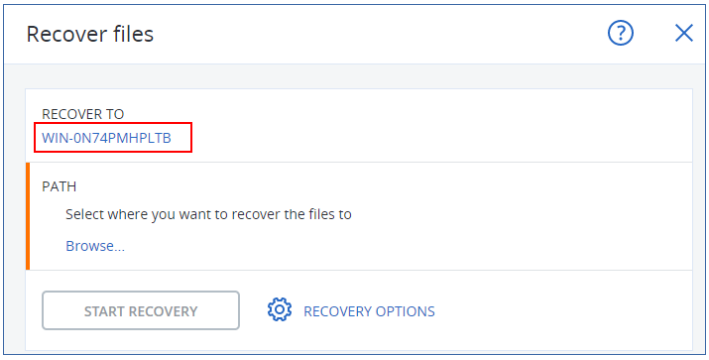
Procedura ta dotyczy komputerów źródłowych w trybie online.

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputer, który pierwotnie zawierał dane do odzyskania, a następnie kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania.

   Punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Bazy danych SQL**, wybierz bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj jako pliki**.
5. [W przypadku odzyskiwania na inny komputer niż pierwotny] W polu **Odzyskaj do** wybierz komputer docelowy.

   Jest to komputer, na który zostaną odzyskane dane. Komputer docelowy musi być w trybie online.

   Aby zmienić wybór, kliknij nazwę komputera, wybierz inny komputer, a następnie kliknij **OK**.



6. W polu **Ścieżka** kliknij **Przeglądaj**, wybierz folder lokalny lub sieciowy, w którym mają zostać

© Acronis International GmbH, 2003-2024

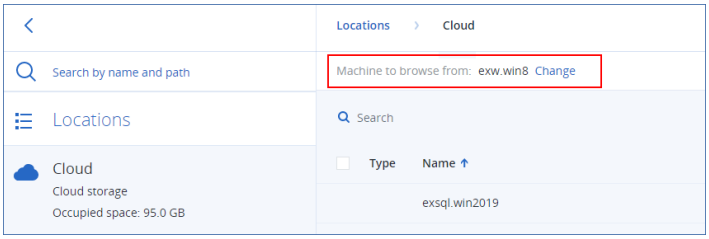
zapisane pliki, a następnie kliknij **Gotowe**.

7. Kliknij **Rozpocznij odzyskiwanie**.

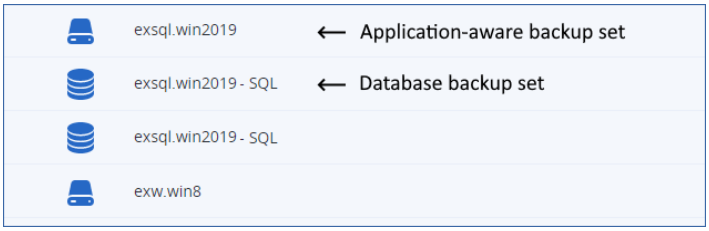
Z kopii zapasowej na komputerze w trybie offline

Ta procedura dotyczy kopii zapasowych uwzględniających aplikacje i kopii zapasowych baz danych zapisanych na komputerach źródłowych, które są w trybie offline.

1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych**.
2. Wybierz lokalizację zestawu kopii zapasowych, z którego chcesz odzyskać dane.
3. W polu **Komputer używany do przeglądania** wybierz komputer docelowy.
   Jest to komputer, na który zostaną odzyskane dane. Komputer docelowy musi być w trybie online.



4. Wybierz zestaw kopii zapasowych, a następnie w panelu **Czynności** kliknij **Pokaż kopie zapasowe**.
   Ikony zestawów kopii zapasowych uwzględniających aplikacje i zestawów kopii zapasowych baz danych różnią się od siebie.



5. Wybierz punkt odzyskiwania, z którego chcesz odzyskać dane.
6. [W przypadku kopii zapasowych baz danych] Kliknij **Odzyskaj bazy danych SQL**.
7. [W przypadku kopii zapasowych uwzględniających aplikacje] Kliknij **Odzyskaj** > **Bazy danych SQL**.
8. Wybierz instancję SQL Server lub kliknij nazwę instancji, aby wybrać bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj jako pliki**.
9. W polu **Ścieżka** kliknij **Przeglądaj**, wybierz folder lokalny lub sieciowy, w którym mają zostać zapisane pliki, a następnie kliknij **Gotowe**.
10. Kliknij **Rozpocznij odzyskiwanie**.

Odzyskiwanie systemowych baz danych

Program odzyska wszystkie systemowe bazy danych instancji jednocześnie. Podczas odzyskiwania systemowych baz danych oprogramowanie automatycznie uruchamia ponownie instancję docelową

© Acronis International GmbH, 2003-2024

w trybie jednego użytkownika. Po zakończeniu odzyskiwania program uruchamia ponownie instancję i odzyskuje pozostałe bazy danych (jeśli występują).

Pozostałe czynniki, które należy uwzględnić podczas odzyskiwania systemowych baz danych:

- Systemowe bazy danych można odzyskać tylko do instancji o takiej samej wersji jak pierwotna instancja.
- Systemowe bazy danych zawsze są odzyskiwane w stanie „gotowe do użycia".

Odzyskiwanie bazy danych master

Systemowe bazy danych obejmują bazę danych **master**. W bazie danych **master** rejestrowane są informacje na temat wszystkich baz danych w danej instancji. Dlatego baza danych **master** w kopii zapasowej zawiera informacje na temat baz danych istniejących w instancji w momencie utworzenia kopii zapasowej. Po odzyskaniu bazy danych **master** konieczne może być wykonanie następujących czynności:

- Bazy danych, które pojawiły się w instancji po utworzeniu kopii zapasowej, nie są dla tej instancji widoczne. Aby umożliwić używanie tych baz danych, dołącz je do instancji ręcznie przy użyciu programu SQL Server Management Studio.
- Bazy danych usunięte po utworzeniu kopii zapasowej są wyświetlane w instancji jako bazy w trybie offline. Usuń je przy użyciu programu SQL Server Management Studio.

Dołączanie baz danych programu SQL Server

W tej sekcji opisano sposób dołączania bazy danych w programie SQL Server za pomocą programu SQL Server Management Studio. W danej chwili może być dołączona tylko jedna baza danych.

Dołączenie bazy danych wymaga posiadania dowolnych z następujących uprawnień: **CREATE DATABASE**, **CREATE ANY DATABASE** lub **ALTER ANY DATABASE**. Zwykle uprawnienia te są przyznawane roli **administratora systemu** w ramach instancji.

Aby dołączyć bazę danych

1. Uruchom program Microsoft SQL Server Management Studio.
2. Podłącz żądaną instancję SQL Server i rozwiń ją.
3. Kliknij prawym przyciskiem myszy **Bazy danych** i kliknij **Dołącz**.
4. Kliknij **Dodaj**.
5. W oknie dialogowym **Odszukaj pliki bazy danych** znajdź i wybierz plik .mdf bazy danych.
6. W sekcji **Szczegóły bazy danych** sprawdź, czy zostały znalezione pozostałe pliki bazy danych (pliki .ndf i .ldf).

   Informacje szczegółowe. Automatyczne znalezienie plików baz danych programu SQL Server może być niemożliwe, jeśli:

   - Nie znajdują się one w lokalizacji domyślnej ani w tym samym folderze co podstawowy plik bazy danych (.mdf). Rozwiązanie: Ręcznie określ ścieżkę do wymaganych plików w kolumnie **Bieżąca ścieżka plików**.

© Acronis International GmbH, 2003-2024

- Odzyskano niekompletny zestaw plików składających się na bazę danych. Rozwiązanie: odzyskaj z kopii zapasowej brakujące pliki bazy danych programu SQL Server.

7. Gdy zostaną znalezione wszystkie pliki, kliknij **OK**.

Odzyskiwanie baz danych programu Exchange

W tej sekcji opisano odzyskiwanie z kopii zapasowych baz danych oraz kopii zapasowych uwzględniających aplikacje.

Dane programu Exchange Server można odzyskać na działający serwer Exchange. Może to być pierwotny serwer Exchange lub serwer Exchange w tej samej wersji działający na komputerze o takiej samej w pełni kwalifikowanej nazwie domeny. Na komputerze docelowym musi być zainstalowany agent dla programu Exchange.

Poniższa tabela zawiera zestawienie danych programu Exchange Server, które można wybrać do odzyskania, oraz minimalne prawa użytkownika wymagane w celu odzyskania tych danych.

Wersja programu Exchange	Elementy danych	Prawa użytkownika
2007	Grupy magazynów	Członkostwo w grupie z rolą **Administratorzy organizacji korzystającej z programu Exchange**.
2010/2013/2016/2019	Bazy danych	Członkostwo w grupie z rolą **Zarządzanie serwerem**.

Można też odzyskać bazy danych (grupy magazynów) jako pliki. Pliki baz danych oraz pliki dzienników transakcji zostaną wyodrębnione z kopii zapasowej do określonego folderu. Może się to przydać, gdy trzeba wyodrębnić dane do inspekcji lub dalszego przetwarzania przez narzędzia innych firm lub gdy odzyskiwanie z jakiegoś powodu się nie powiodło i potrzebny jest sposób na ręczne zamontowanie baz danych.

Jeśli używasz tylko agenta dla VMware (system Windows), jedyną dostępną metodą odzyskiwania jest odzyskiwanie baz danych jako plików. Nie można odzyskiwać baz danych za pomocą agenta dla VMware (urządzenie wirtualne).

W przypadku poniższych procedur pojęcie „bazy danych” dotyczy zarówno baz danych, jak i grup magazynów.

Aby odzyskać bazy danych programu Exchange do działającego programu Exchange Server

1. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft Exchange** > **Bazy danych**, a następnie wybierz bazy danych, które chcesz odzyskać.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

© Acronis International GmbH, 2003-2024

Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj jedną z następujących czynności:

- [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacja kopii zapasowej to chmura lub współużytkowany magazyn (czyli inni agenci mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange będący w trybie online, a następnie wybierz punkt odzyskiwania.
- Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania danych programu Exchange.

4. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje kliknij **Odzyskaj** > **Bazy danych programu Exchange**, wybierz bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij opcję **Odzyskaj** > **Bazy danych do serwera programu Exchange**.
5. Domyślnie program odzyska bazy danych do pierwotnej lokalizacji. Jeśli pierwotna baza danych nie istnieje, zostanie odtworzona.

   Aby odzyskać bazę danych jako inną bazę danych:

   a. Kliknij nazwę bazy danych.

   b. W polu **Odzyskaj do** wybierz **Nowa baza danych**.

   c. Określ nazwę nowej bazy danych.

   d. Określ ścieżkę nowej bazy danych oraz ścieżkę dziennika. Określony tutaj folder nie może zawierać pierwotnej bazy danych ani plików dziennika.
6. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie Działania jest wyświetlany postęp odzyskiwania.

Aby odzyskać bazy danych programu Exchange jako pliki

1. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft Exchange** > **Bazy danych**, a następnie wybierz bazy danych, które chcesz odzyskać.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj jedną z następujących czynności:

   - [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacją kopii zapasowej jest chmura lub współużytkowany magazyn (czyli inne agenty mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange lub agentem dla VMware będący w trybie online, a następnie wybierz punkt

© Acronis International GmbH, 2003-2024

odzyskiwania.

- Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania danych programu Exchange.

4. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje kliknij **Odzyskaj** > **Bazy danych programu Exchange**, wybierz bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj jako pliki**.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Odzyskaj** > **Bazy danych jako pliki**.
5. Kliknij **Przeglądaj**, a następnie wybierz folder lokalny lub sieciowy, w którym mają zostać zapisane pliki.
6. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie Działania jest wyświetlany postęp odzyskiwania.

Montowanie baz danych programu Exchange Server

Po odzyskaniu plików baz danych można udostępnić bazy danych w trybie online, montując je. Montowanie przeprowadza się za pomocą konsoli Exchange Management Console, menedżera Exchange System Manager lub powłoki Exchange Management Shell.

Odzyskane bazy danych będą się znajdować w stanie „nieprawidłowego zamknięcia systemu". Bazę danych będącą w stanie „nieprawidłowego zamknięcia systemu" może zamontować, jeśli zostanie ona odzyskana do oryginalnej lokalizacji (informacje o oryginalnej bazie danych są obecne w usłudze Active Directory). W przypadku odzyskiwania bazy danych do innej lokalizacji (takiej jak nowa baza danych lub baza danych odzyskiwania) jej zamontowanie jest możliwe dopiero po przywróceniu jej do stanu „czystego zamknięcia" za pomocą polecenia `Eseutil /r <Enn>`. Nazwa `<Enn>` określa prefiks pliku dziennika bazy danych (lub grupy magazynów zawierającej bazę danych), względem którego należy zastosować pliki dziennika transakcji.

Konto używane do dołączania bazy danych musi mieć delegowaną rolę administratora programu Exchange Server i lokalną grupę Administratorzy serwera docelowego.

Aby uzyskać więcej informacji na temat montowania baz danych, zobacz następujące artykuły:

- Program Exchange w wersji 2010 lub nowszej: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Program Exchange w wersji 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

© Acronis International GmbH, 2003-2024

Odzyskiwanie skrzynek pocztowych programu Exchange i ich elementów

Skrzynki pocztowe programu Exchange i ich elementy można odzyskiwać z następujących kopii zapasowych:

- Kopie zapasowe baz danych
- Kopie zapasowe uwzględniające aplikacje
- Kopie zapasowe skrzynek pocztowych

Można odzyskiwać następujące elementy:

- Skrzynki pocztowe (z wyjątkiem archiwalnych skrzynek pocztowych)
- Foldery publiczne

> **Uwaga**
> Dostępne tylko z kopii zapasowych baz danych. Zobacz "Wybieranie danych programu Exchange Server" (s. 604).

- Elementy folderu publicznego
- Foldery poczty e-mail
- Wiadomości e-mail
- Zdarzenia kalendarza
- Zadania
- Kontakty
- Wpisy dziennika
- Notatki

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

Skrzynki pocztowe lub elementy skrzynek pocztowych można odzyskać na aktywny serwer Exchange Server lub do usługi Microsoft 365.

Odzyskiwanie na serwer Exchange Server

Odzyskiwanie granularne jest możliwe tylko w przypadku programu Microsoft Exchange Server 2010 z dodatkiem Service Pack 1 (SP1) lub nowszego. Źródłowa kopia zapasowa może zawierać bazy danych lub skrzynki pocztowe dowolnej obsługiwanej wersji programu Exchange.

Odzyskiwanie granularne może wykonać agent dla programu Exchange lub agent dla VMware (w systemie Windows). Docelowy komputer z programem Exchange Server oraz komputer z uruchomionym agentem muszą się znajdować w tym samym lesie usługi Active Directory.

© Acronis International GmbH, 2003-2024

W przypadku odzyskiwania skrzynki pocztowej do już istniejącej skrzynki dostępne w niej elementy o takich samych identyfikatorach zostaną zastąpione.

Odzyskiwanie elementów skrzynki pocztowej nie powoduje zastępowania żadnych danych. Zamiast tego w folderze docelowym zostanie odtworzona pełna ścieżka elementu skrzynki pocztowej.

Wymagania dotyczące kont użytkowników

Odzyskiwana z kopii zapasowej skrzynka pocztowa musi mieć powiązane konto użytkownika w usłudze Active Directory.

Skrzynki pocztowe użytkowników i ich zawartość można odzyskać tylko pod warunkiem, że są *włączone* powiązane z nimi konta użytkowników. Współdzielone skrzynki pocztowe oraz skrzynki pocztowe pomieszczeń i urządzeń można odzyskać pod warunkiem, że powiązane z nimi konta użytkowników są *wyłączone*.

Skrzynki pocztowe, które nie spełniają powyższych warunków, są pomijane podczas odzyskiwania.

W przypadku pominięcia niektórych skrzynek pocztowych odzyskiwanie zakończy się powodzeniem z ostrzeżeniami. W przypadku pominięcia wszystkich skrzynek pocztowych odzyskiwania zakończy się niepowodzeniem.

Odzyskiwanie do usługi Microsoft 365

Odzyskiwanie elementów danych programu Exchange do usługi Microsoft 365 i na odwrót jest obsługiwane pod warunkiem, że lokalnie jest zainstalowany agent dla usługi Microsoft 365.

Odzyskiwanie jest możliwe tylko w przypadku kopii zapasowych programu Microsoft Exchange Server 2010 lub nowszego.

W przypadku odzyskiwania skrzynki pocztowej do istniejącej już skrzynki Microsoft 365 dostępne w niej elementy pozostają niezmienione, a odzyskane elementy zostają po prostu dodane.

W przypadku odzyskiwania jednej skrzynki pocztowej należy wybrać docelową skrzynkę pocztową Microsoft 365. W przypadku odzyskiwania kilku skrzynek pocztowych w ramach jednej operacji program spróbuje odzyskać każdą skrzynkę do skrzynki użytkownika o tej samej nazwie. W razie nieznalezienia danego użytkownika skrzynka pocztowa zostanie pominięta. W przypadku pominięcia niektórych skrzynek pocztowych odzyskiwanie zakończy się powodzeniem z ostrzeżeniami. W przypadku pominięcia wszystkich skrzynek pocztowych odzyskiwania zakończy się niepowodzeniem.

Dodatkowe informacje na temat odzyskiwania do usługi Microsoft 365 można znaleźć w sekcji "Ochrona danych Microsoft 365" (s. 641).

Odzyskiwanie skrzynek pocztowych

Aby odzyskać skrzynki pocztowe z kopii zapasowej uwzględniającej aplikacje lub kopii zapasowej bazy danych

1. [Tylko w przypadku odzyskiwania z kopii zapasowej bazy danych do usługi Microsoft 365] Jeśli na komputerze z programem Exchange Server uwzględnianym w kopii zapasowej nie jest

© Acronis International GmbH, 2003-2024

zainstalowany agent dla usługi Microsoft 365, wykonaj jedną z następujących czynności:

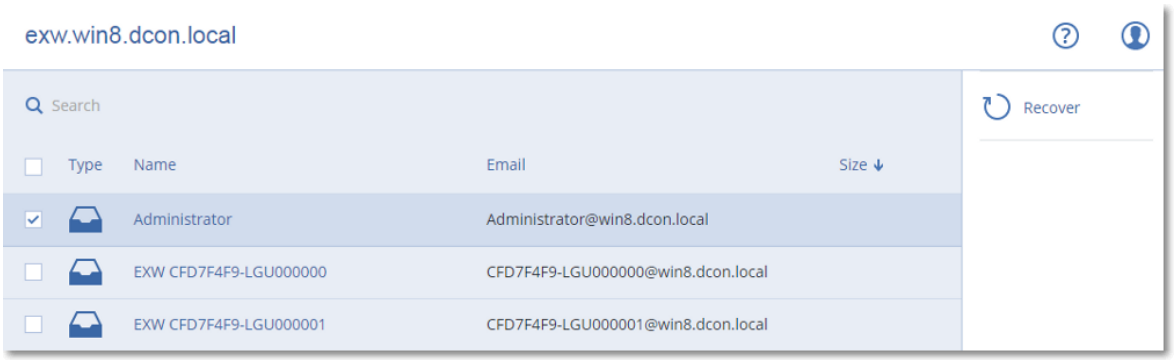
- Jeśli w Twojej organizacji nie ma agenta dla usługi Microsoft 365, zainstaluj go na komputerze uwzględnionym w kopii zapasowej (lub innym komputerze z tą samą wersją programu Microsoft Exchange Server).
- Jeśli w organizacji już jest agent dla usługi Microsoft 365, skopiuj biblioteki z komputera uwzględnionego w kopii zapasowej (lub innego komputera z tą samą wersją programu Microsoft Exchange Server) na komputer z tym agentem, postępując zgodnie z opisem podanym w sekcji „Kopiowanie bibliotek programu Microsoft Exchange”.

2. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft Exchange** > **Bazy danych**, a następnie wybierz bazę danych pierwotnie zawierającą dane, które chcesz odzyskać.
3. Kliknij **Odzyskiwanie**.
4. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Skorzystaj z innych metod odzyskiwania:
   - [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacją kopii zapasowej jest chmura lub współużytkowany magazyn (czyli inne agenty mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange lub agentem dla VMware będący w trybie online, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

   Komputer wybrany do przejrzenia w ramach dowolnego z powyższych działań wykona operację odzyskiwania w zastępstwie pierwotnego komputera będącego w trybie offline.
5. Kliknij **Odzyskaj** > **Skrzynki pocztowe programu Exchange**.
6. Wybierz skrzynki pocztowe, które chcesz odzyskać.

   Skrzynki pocztowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.



7. Kliknij **Odzyskaj**.
8. [Tylko w przypadku odzyskiwania do usługi Microsoft 365]:

© Acronis International GmbH, 2003-2024

a. W polu **Odzyskaj do** wybierz **Microsoft 365**.

b. [Jeśli w kroku 6 została wybrana tylko jedna skrzynka pocztowa] W polu **Docelowa skrzynka pocztowa** określ docelową skrzynkę pocztową.

c. Kliknij **Rozpocznij odzyskiwanie**.

Kolejne kroki tej procedury nie są wymagane.

Kliknij **Komputer docelowy z programem Microsoft Exchange Server**, aby wybrać lub zmienić komputer docelowy. Dzięki temu można odzyskać dane na komputer bez agenta dla programu Exchange.

Podaj w pełni kwalifikowaną nazwę domeny (FQDN) komputera, na którym jest włączona rola **Dostęp klienta** (w przypadku programu Microsoft Exchange Server 2010/2013) lub **rola Skrzynka pocztowa** (w przypadku programu Microsoft Exchange Server 2016 lub nowszego). Komputer musi należeć do tego samego lasu usługi Active Directory co komputer wykonujący operację odzyskiwania.

9. Jeśli pojawi się stosowny monit, określ poświadczenia konta, które będzie używane w celu uzyskania dostępu do komputera. Wymagania wobec takiego konta znajdują się w sekcji „Wymagane prawa użytkownika".
10. [Opcjonalnie] Kliknij **Baza danych używana do odtworzenia brakujących skrzynek pocztowych**, aby zmienić automatycznie wybraną bazę danych.
11. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby odzyskać skrzynkę pocztową z kopii zapasowej skrzynek pocztowych

1. Kliknij kolejno **Urządzenia** > **Microsoft Exchange** > **Skrzynki pocztowe**.
2. Wybierz skrzynkę pocztową do odzyskania, a następnie kliknij **Odzyskiwanie**.

   Skrzynki pocztowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.

   Jeśli skrzynka pocztowa została usunięta, zaznacz ją na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
3. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Skrzynka pocztowa**.
5. Wykonaj kroki 8–11 powyższej procedury.

Odzyskiwanie elementów skrzynki pocztowej

Aby odzyskać elementy skrzynki pocztowej z kopii zapasowej uwzględniającej aplikacje lub kopii zapasowej bazy danych

1. [Tylko w przypadku odzyskiwania z kopii zapasowej bazy danych do usługi Microsoft 365] Jeśli na komputerze z programem Exchange Server uwzględnianym w kopii zapasowej nie jest zainstalowany agent dla usługi Microsoft 365, wykonaj jedną z następujących czynności:
   - Jeśli w Twojej organizacji nie ma agenta dla usługi Microsoft 365, zainstaluj go na komputerze uwzględnionym w kopii zapasowej (lub innym komputerze z tą samą wersją programu Microsoft Exchange Server).

© Acronis International GmbH, 2003-2024

- Jeśli w organizacji już jest agent dla usługi Microsoft 365, skopiuj biblioteki z komputera uwzględnionego w kopii zapasowej (lub innego komputera z tą samą wersją programu Microsoft Exchange Server) na komputer z tym agentem, postępując zgodnie z opisem podanym w sekcji „Kopiowanie bibliotek programu Microsoft Exchange".

2. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft Exchange** > **Bazy danych**, a następnie wybierz bazę danych pierwotnie zawierającą dane, które chcesz odzyskać.
3. Kliknij **Odzyskiwanie**.
4. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji. Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Skorzystaj z innych metod odzyskiwania:
   - [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacją kopii zapasowej jest chmura lub współużytkowany magazyn (czyli inne agenty mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange lub agentem dla VMware będący w trybie online, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

   Komputer wybrany do przejrzenia w ramach dowolnego z powyższych działań wykona operację odzyskiwania w zastępstwie pierwotnego komputera będącego w trybie offline.
5. Kliknij **Odzyskaj** > **Skrzynki pocztowe programu Exchange**.
6. Kliknij skrzynkę pocztową, która pierwotnie zawierała elementy do odzyskania.
7. Wybierz elementy, które chcesz odzyskać.

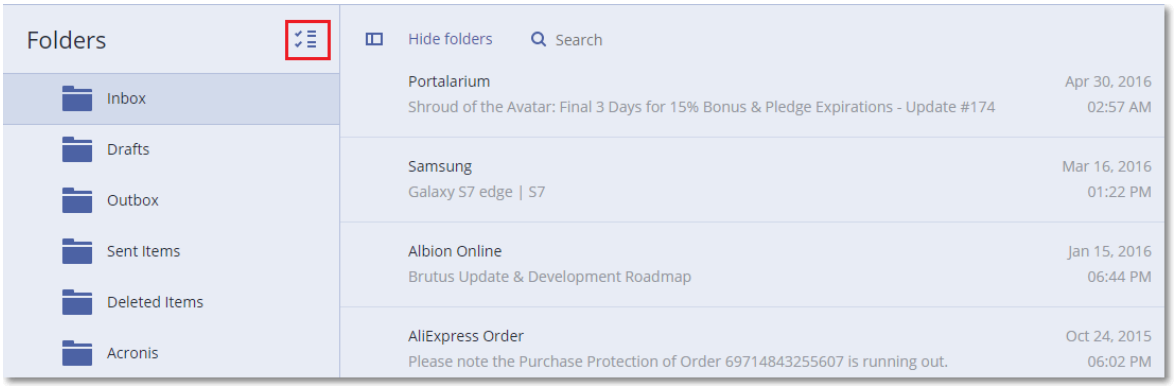
   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.
   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata i daty.
   - Zdarzenia: wyszukiwanie według tematu i daty.
   - Zadania: wyszukiwanie według tematu i daty.
   - Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.

   Po zaznaczeniu wiadomości e-mail możesz kliknąć **Pokaż zawartość**, aby wyświetlić jej zawartość, w tym załączniki.

   Uwaga
   Kliknij nazwę załączonego pliku, aby go pobrać.

   Aby mieć możliwość wybrania folderów, kliknij ikonę odzyskiwania folderów.

© Acronis International GmbH, 2003-2024



8. Kliknij **Odzyskaj**.
9. Aby odzyskać do usługi Microsoft 365, wybierz **Microsoft 365** w polu **Odzyskaj do**.

   Aby odzyskać na serwer Exchange Server, zachowaj wartość domyślną **Microsoft Exchange** w polu **Odzyskaj do**.

   [Tylko w przypadku odzyskiwania na serwer Exchange Server] Kliknij **Komputer docelowy z programem Microsoft Exchange Server**, aby wybrać lub zmienić komputer docelowy. Dzięki temu można odzyskać dane na komputer bez agenta dla programu Exchange.

   Podaj w pełni kwalifikowaną nazwę domeny (FQDN) komputera, na którym jest włączona rola **Dostęp klienta** (w przypadku programu Microsoft Exchange Server 2010/2013) lub **rola Skrzynka pocztowa** (w przypadku programu Microsoft Exchange Server 2016 lub nowszego). Komputer musi należeć do tego samego lasu usługi Active Directory co komputer wykonujący operację odzyskiwania.
10. Jeśli pojawi się stosowny monit, określ poświadczenia konta, które będzie używane w celu uzyskania dostępu do komputera. Wymagania wobec takiego konta znajdują się w sekcji „Wymagane prawa użytkownika”.
11. W polu **Docelowa skrzynka pocztowa** wyświetl, zmień lub określ docelową skrzynkę pocztową.

    Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano komputer inny niż pierwotny, trzeba określić docelową skrzynkę pocztową.
12. [Tylko w przypadku odzyskiwania wiadomości e-mail] W polu **Folder docelowy** wyświetl lub zmień folder docelowy w docelowej skrzynce pocztowej. Domyślnie wybrany jest folder **Odzyskane elementy**. Ze względu na ograniczenia programu Microsoft Exchange zdarzenia, zadania, notatki i kontakty są przywracane do pierwotnej lokalizacji, nawet jeśli w polu **Folder docelowy** podano inną lokalizację.
13. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby odzyskać skrzynkę pocztową z kopii zapasowej skrzynek pocztowych

1. Kliknij kolejno **Urządzenia** > **Microsoft Exchange** > **Skrzynki pocztowe**.
2. Wybierz skrzynkę pocztową, która pierwotnie zawierała elementy do odzyskania, a następnie kliknij **Odzyskiwanie**.

   Skrzynki pocztowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.

© Acronis International GmbH, 2003-2024

Jeśli skrzynka pocztowa została usunięta, zaznacz ją na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

3. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
5. Wybierz elementy, które chcesz odzyskać.

   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.

   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata i daty.
   - Zdarzenia: wyszukiwanie według tematu i daty.
   - Zadania: wyszukiwanie według tematu i daty.
   - Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.

   Po zaznaczeniu wiadomości e-mail możesz kliknąć **Pokaż zawartość**, aby wyświetlić jej zawartość, w tym załączniki.

   Uwaga
   Kliknij nazwę załączonego pliku, aby go pobrać.

   Po zaznaczeniu wiadomości e-mail możesz kliknąć **Wyślij jako wiadomość e-mail**, aby wysłać wiadomość na jakiś adres e-mail. Wiadomość zostanie wysłana z adresu email konta administratora.

   Aby mieć możliwość wybrania folderów, kliknij ikonę odzyskiwania folderów:
6. Kliknij **Odzyskaj**.
7. Wykonaj kroki 9–13 powyższej procedury.

Kopiowanie bibliotek programu Microsoft Exchange Server

W przypadku odzyskiwania skrzynek pocztowych programu Exchange lub ich elementów do usługi Microsoft 365 może być konieczne skopiowanie poniższych bibliotek z komputera uwzględnionego w kopii zapasowej (lub innego komputera z tą samą wersją programu Microsoft Exchange Server) na komputer z agentem dla usługi Microsoft 365.

Skopiuj poniższe pliki, zgodnie z wersją programu Microsoft Exchange Server uwzględnioną w kopii zapasowej.

Wersja serwera Microsoft Exchange Server	Biblioteki	Lokalizacja domyślna

Microsoft Exchange Server 2010	`ese.dll`
	`esebcli2.dll`
	`store.exe`
		`%ProgramFiles%\Microsoft\Exchange Server\V14\bin`

Microsoft Exchange Server 2013	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`

© Acronis International GmbH, 2003-2024

	`msvcr110.dll`	`%WINDIR%\system32`
Microsoft Exchange Server 2016, 2019	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll` `msvcp110.dll`	`%WINDIR%\system32`

Biblioteki powinny zostać umieszczone w folderze `%ProgramData%\Acronis\ese`. Jeśli taki folder nie istnieje, utwórz go ręcznie.

Zmiana poświadczeń dostępu programu SQL Server lub Exchange Serwer

Możesz zmienić poświadczenia dostępu dla programu SQL Server lub Exchange Server bez ponownej instalacji agenta.

Aby zmienić poświadczenia dostępu programu SQL Server lub Exchange Serwer

1. Kliknij **Urządzenia**, a następnie kliknij **Microsoft SQL** lub **Microsoft Exchange**.
2. Wybierz zawsze włączoną grupę dostępności, grupę dostępności bazy danych, instancję SQL Server lub serwer Exchange, w których przypadku chcesz zmienić poświadczenia dostępu.
3. Kliknij **Określ poświadczenia**.
4. Określ nowe poświadczenia dostępu, a następnie kliknij **OK**.

Aby zmienić poświadczenia dostępu serwera Exchange Serwer dla kopii zapasowej skrzynki pocztowej

1. Kliknij **Urządzenia** > **Microsoft Exchange** i rozwiń węzeł **Skrzynki pocztowe**.
2. Wybierz program Exchange Server, dla którego chcesz zmienić poświadczenia dostępu.
3. Kliknij **Ustawienia**.
4. W obszarze **Konto administratora programu Exchange** określ nowe poświadczenia dostępu, a następnie kliknij **Zapisz**.

Ochrona urządzeń mobilnych

Aplikacja Acronis Cyber Protect umożliwia utworzenie kopii zapasowych danych z urządzenia mobilnego w chmurze, a następnie odzyskanie tych danych w razie ich utraty lub uszkodzenia. Uwaga: tworzenie kopii zapasowych w chmurze wymaga konta i subskrypcji chmury Cloud.

Obsługiwane urządzenia mobilne

Aplikację Cyber Protect można zainstalować na urządzeniu mobilnym z jednym z następujących systemów operacyjnych:

© Acronis International GmbH, 2003-2024

- od iOS 15 do iOS 17 (iPhone, iPod, iPad)
- od Android 10 do Android 14

Elementy, które można uwzględnić w kopii zapasowej

- Kontakty (imię i nazwisko, numer telefonu oraz adres e-mail)
- Zdjęcia (zachowywany jest oryginalny rozmiar i format zdjęć)
- Wideo
- Kalendarze
- Przypomnienia (tylko na urządzeniach z systemem iOS)

Co trzeba wiedzieć

- Kopie zapasowe danych można tworzyć tylko w chmurze.
- Po każdym otwarciu aplikacji pojawi się podsumowanie zmian w danych i będzie można ręcznie rozpocząć tworzenie kopii zapasowej.
- Funkcja **Ciągła kopia zapasowa** jest domyślnie włączona. Jeśli to ustawienie jest włączone, aplikacja Cyber Protect automatycznie i na bieżąco wykrywa nowe dane oraz przesyła je do środowiska Cloud.
- Opcja **Używaj tylko połączenia Wi-Fi** jest domyślnie włączona w ustawieniach aplikacji. Jeśli to ustawienie jest włączone, aplikacja Cyber Protect będzie tworzyć kopię zapasową danych tylko wtedy, gdy będzie dostępne połączenie Wi-Fi. W przypadku braku połączenia Wi-Fi tworzenie kopii zapasowej nie zostanie rozpoczęte. Jeśli aplikacja ma korzystać również z połączenia przez sieć telefonii komórkowej, wyłącz tę opcję.
- Funkcja optymalizacji działania baterii urządzenia może uniemożliwiać prawidłowe działanie aplikacji Cyber Protect. Aby operacje tworzenia kopii zapasowych były uruchamiane na czas, należy zatrzymać optymalizację działania baterii w przypadku danej aplikacji.
- Można oszczędzać energię na dwa sposoby:
  - Funkcja **Twórz kopię podczas ładowania** jest domyślnie wyłączona. Jeśli to ustawienie jest włączone, aplikacja Cyber Protect będzie tworzyć kopię zapasową danych tylko wtedy, gdy urządzenie jest podłączone do źródła zasilania. W przypadku odłączenia urządzenia od źródła zasilania podczas tworzenia ciągłej kopii zapasowej operacja ta zostanie wstrzymana.
  - Przy użyciu opcji **Tryb energooszczędny**, która jest domyślnie włączona. Jeśli to ustawienie jest włączone, aplikacja Cyber Protect będzie tworzyć kopię zapasową danych tylko wtedy, gdy stan naładowania baterii nie jest niski. Gdy stan naładowania baterii będzie niski, tworzenie ciągłej kopii zapasowej zostanie wstrzymane.
- Dane z kopii zapasowej są dostępne na każdym urządzeniu mobilnym zarejestrowanym na danym koncie. Dzięki temu można łatwiej przenosić dane ze starego urządzenia mobilnego na nowe. Kontakty i zdjęcia z urządzenia z systemem Android można odzyskać na urządzenie z systemem iOS — i na odwrót. Zdjęcie, film lub kontakt można też pobrać na dowolne urządzenie za pomocą konsoli Cyber Protect.

© Acronis International GmbH, 2003-2024

- Uwzględnione w kopii zapasowej dane z urządzenia mobilnego zarejestrowanego na koncie są widoczne tylko na tym koncie. Nikt inny nie może wyświetlić ani odzyskać Twoich danych.
- W aplikacji Cyber Protect można odzyskać tylko najnowszą wersję danych. Jeśli potrzebujesz odzyskać dane z określonej wersji kopii zapasowej, skorzystaj z konsoli Cyber Protect na tablecie lub komputerze.
- W przypadku kopii zapasowych urządzeń mobilnych reguły przechowywania nie mają zastosowania.
- [Tylko w przypadku urządzeń z systemem Android] Jeśli podczas tworzenia kopii zapasowej w urządzeniu znajduje się karta SD, w kopii zapasowej zostaną uwzględnione również dane z tej karty. Dane te zostaną odzyskane do folderu **Odzyskano przy użyciu kopii zapasowej** na karcie SD, jeśli jest ona dostępna podczas odzyskiwania, lub aplikacja wyświetli monit o wskazanie innej lokalizacji, do której mają zostać odzyskane dane.

Jak uzyskać aplikację Cyber Protect

W zależności od urządzenia mobilnego zainstaluj aplikację ze sklepu App Store lub Google Play.

Jak rozpocząć tworzenie kopii zapasowej danych

1. Otwórz aplikację.
2. Zaloguj się przy użyciu swojego konta.
3. Stuknij **Skonfiguruj**, aby utworzyć kopię zapasową. Uwaga: ten przycisk jest wyświetlany tylko wtedy, gdy nie ma jeszcze żadnej kopii zapasowej urządzenia mobilnego.
4. Wybierz kategorie danych, które chcesz uwzględnić w kopii zapasowej. Domyślnie wybrane są wszystkie kategorie.
5. [Opcjonalnie] Włącz opcję **Szyfruj kopię zapasową**, aby chronić kopię zapasową przez jej zaszyfrowanie. W takim przypadku trzeba będzie również:
   a. Dwa razy wprowadzić hasło szyfrowania.

      Uwaga
      Dobrze zapamiętać hasło, ponieważ zapomnianego hasła nie da się przywrócić ani zmienić.

   b. Stuknij **Szyfruj**.
6. Stuknij **Utwórz kopię zapasową**.
7. Zezwól aplikacji na dostęp do Twoich danych osobistych. Jeśli odmówisz dostępu do niektórych kategorii danych, nie będą one uwzględniane w kopiach zapasowych.

Rozpocznie się operacja tworzenia kopii zapasowych.

Jak odzyskać dane na urządzenie mobilne

Ostrzeżenie!
Aby odzyskać dane mobilne, trzeba użyć konta użytkownika.

© Acronis International GmbH, 2003-2024

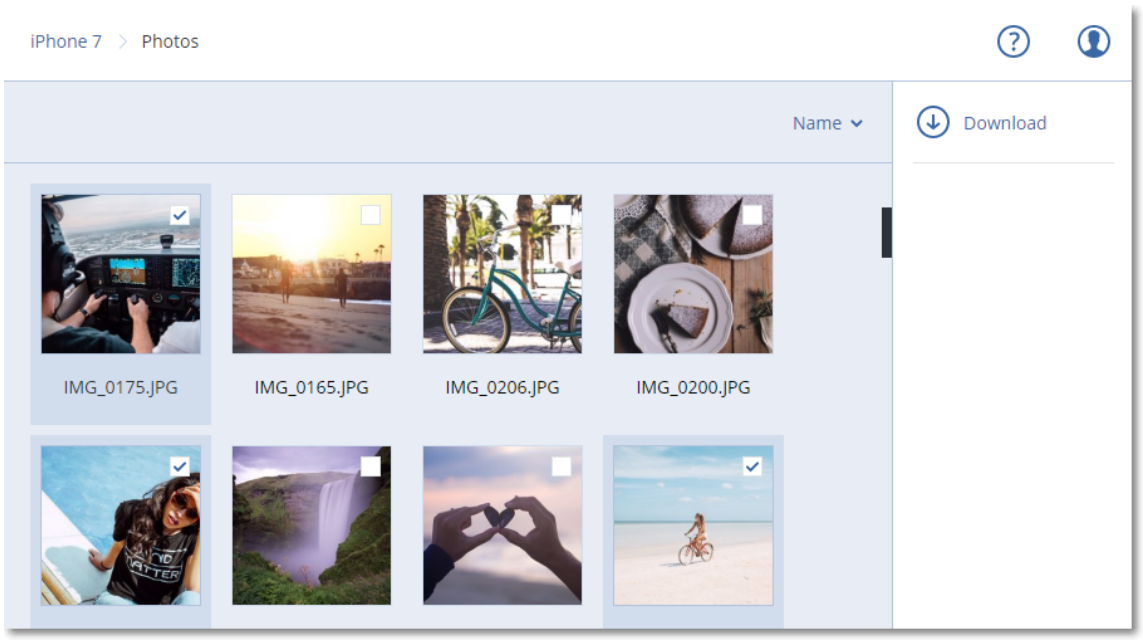
1. Otwórz aplikację Cyber Protect.
2. Stuknij **Przeglądaj**.
3. Stuknij nazwę urządzenia.
4. Wykonaj jedną z następujących czynności:
   - Aby odzyskać wszystkie dane z kopii zapasowej, stuknij **Odzyskaj wszystko**. Nie trzeba wykonywać żadnych innych czynności.
   - Aby odzyskać tylko wybrane kategorie danych, stuknij **Wybierz**, a następnie stuknij pola wyboru wymaganych kategorii danych. Stuknij **Odzyskaj**. Nie trzeba wykonywać żadnych innych czynności.
   - Aby odzyskać tylko wybrane elementy danych należące do tej samej kategorii danych, stuknij odpowiednią kategorię danych. Przejdź do kolejnych działań.
5. Wykonaj jedną z następujących czynności:
   - Aby odzyskać jeden element danych, stuknij go.
   - Aby odzyskać kilka elementów danych, stuknij **Wybierz**, a następnie stuknij pola wyboru wymaganych elementów danych.
6. Stuknij **Odzyskaj**.

Jak przeglądać dane za pomocą konsoli Cyber Protect

1. Na komputerze otwórz przeglądarkę i wpisz adres URL konsoli Cyber Protect.
2. Zaloguj się przy użyciu swojego konta.
3. W obszarze **Wszystkie urządzenia** kliknij **Odzyskaj** pod nazwą urządzenia mobilnego.
4. Wykonaj dowolne z następujących czynności:
   - Aby pobrać wszystkie zdjęcia, filmy, kontakty, kalendarze lub przypomnienia, wybierz odpowiednią kategorię danych. Kliknij **Pobierz**.

© Acronis International GmbH, 2003-2024

- Aby pobrać wybrane zdjęcia, filmy, kontakty, kalendarze lub przypomnienia, kliknij nazwę odpowiedniej kategorii danych, a następnie zaznacz pola wyboru obok potrzebnych elementów danych. Kliknij **Pobierz**.



- Aby wyświetlić zdjęcie lub kontakt, kliknij nazwę odpowiedniej kategorii danych, a następnie kliknij wymagany element danych.

Chronienie danych usługi Hosted Exchange

Jakie elementy można uwzględnić w kopii zapasowej?

W kopii zapasowej można uwzględnić skrzynki pocztowe użytkowników i grup oraz skrzynki współdzielone. Opcjonalnie można wybrać tworzenie kopii zapasowej archiwalnych skrzynek pocztowych (**archiwum zbiorczego**) dla wybranych skrzynek.

Jakie elementy można odzyskać?

Z kopii zapasowej skrzynek pocztowych można odzyskać następujące elementy:

- Skrzynki pocztowe
- Foldery poczty e-mail
- Wiadomości e-mail
- Zdarzenia kalendarza
- Zadania
- Kontakty
- Wpisy dziennika
- Notatki

© Acronis International GmbH, 2003-2024

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

Odzyskując skrzynki pocztowe, elementy skrzynek pocztowych, foldery publiczne i elementy folderów publicznych, można wybrać, czy elementy w lokalizacji docelowej mają zostać zastąpione.

W przypadku odzyskiwania skrzynki pocztowej do już istniejącej skrzynki dostępne w niej elementy o takich samych identyfikatorach zostaną zastąpione.

Odzyskiwanie elementów skrzynki pocztowej nie powoduje zastępowania żadnych danych. Zamiast tego w folderze docelowym zostanie odtworzona pełna ścieżka elementu skrzynki pocztowej.

Wybieranie skrzynek pocztowych programu Exchange Online

Wybierz skrzynki pocztowe zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać skrzynki pocztowe programu Exchange Online

1. Kliknij **Urządzenia > Hosted Exchange**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Hosted Exchange, wybierz tę organizację, w której przypadku chcesz utworzyć kopię zapasową danych użytkowników. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby tworzyć kopie zapasowe wszystkich skrzynek pocztowych użytkowników i wszystkich skrzynek współdzielonych (w tym skrzynek, które zostaną utworzone w przyszłości), rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby tworzyć kopie zapasowe wybranych skrzynek pocztowych użytkowników lub skrzynek współdzielonych, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wybierz użytkowników, których skrzynki pocztowe chcesz uwzględniać w kopiach zapasowych, i kliknij **Kopia zapasowa**.
   - Aby tworzyć kopie zapasowe skrzynek pocztowych wszystkich grup (w tym skrzynek, które zostaną utworzone w przyszłości), rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby tworzyć kopie zapasowe wybranych grupowych skrzynek pocztowych, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, następnie wskaż grupy, dla których chcesz wykonać kopię zapasową skrzynek pocztowych, po czym kliknij **Kopia zapasowa**.

© Acronis International GmbH, 2003-2024

Odzyskiwanie skrzynek pocztowych i elementów skrzynek pocztowych

Odzyskiwanie skrzynek pocztowych

1. Kliknij **Urządzenia > Hosted Exchange**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Hosted Exchange, wybierz tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby odzyskać skrzynkę pocztową użytkownika, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż użytkownika, którego skrzynkę pocztową chcesz odzyskać, po czym kliknij **Odzyskiwanie**.
   - Aby odzyskać współdzieloną skrzynkę pocztową, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż skrzynkę współdzieloną, którą chcesz odzyskać, i kliknij **Odzyskiwanie**.
   - Aby odzyskać skrzynkę pocztową grupy, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie wskaż grupę, której skrzynkę pocztową chcesz odzyskać, po czym kliknij **Odzyskiwanie**.
   - Jeśli skrzynka pocztowa użytkownika, grupy lub współdzielona została usunięta, wybierz element w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

   Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Cała skrzynka pocztowa**.
6. Jeśli do usługi Cyber Protection dodano wiele organizacji Hosted Exchange, kliknij **Organizacja usługi Hosted Exchange**, aby wyświetlić, zmienić lub określić organizację docelową.

   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
7. W polu **Odzyskaj do skrzynki pocztowej** wyświetl, zmień lub określ docelową skrzynkę pocztową.

   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelową skrzynkę pocztową.
8. Kliknij **Rozpocznij odzyskiwanie**.
9. Wybierz jedną z następujących opcji zastępowania:
   - **Zastąp istniejące elementy**
   - **Nie zastępuj istniejących elementów**
10. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

© Acronis International GmbH, 2003-2024

Odzyskiwanie elementów skrzynki pocztowej

1. Kliknij **Urządzenia > Hosted Exchange**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Hosted Exchange, wybierz tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby odzyskać elementy ze skrzynki pocztowej użytkownika, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż użytkownika, którego skrzynka pocztowa pierwotnie zawierała elementy do odzyskania, po czym kliknij **Odzyskiwanie**.
   - Aby odzyskać elementy ze współdzielonej skrzynki pocztowej, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż skrzynkę współdzieloną pierwotnie zawierającą elementy, które chcesz odzyskać, i kliknij **Odzyskiwanie**.
   - Aby odzyskać elementy ze skrzynki pocztowej grupy, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie wskaż grupę, której skrzynka pocztowa pierwotnie zawierała elementy do odzyskania, po czym kliknij **Odzyskiwanie**.
   - Jeśli skrzynka pocztowa użytkownika, grupy lub współdzielona została usunięta, wybierz element w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

   Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
6. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów.

   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.
   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata, nazwy załącznika i daty.
   - Zdarzenia: wyszukiwanie według tematu i daty.
   - Zadania: wyszukiwanie według tematu i daty.
   - Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.
7. Wybierz elementy, które chcesz odzyskać. Aby mieć możliwość wybrania folderów, kliknij ikonę „Odzyskaj foldery”:

   Możesz również wykonać dowolną z następujących czynności:
   - Po wybraniu elementu kliknij **Pokaż zawartość**, aby zobaczyć jego zawartość, w tym załączniki. Kliknij nazwę załączonego pliku, aby go pobrać.
   - Po zaznaczeniu wiadomości e-mail lub elementu kalendarza możesz kliknąć **Wyślij jako wiadomość e-mail**, aby wysłać ten element na wskazany adres e-mail. Możesz wybrać nadawcę i napisać tekst, który zostanie dołączony do przekazywanego elementu.
   - Tylko w sytuacji, gdy kopia zapasowa nie jest zaszyfrowana, a w wynikach wyszukiwania wybrano jeden element: kliknij **Pokaż wersje**, aby wybrać wersję elementu do odzyskania.

© Acronis International GmbH, 2003-2024

Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.

8. Kliknij **Odzyskaj**.
9. Jeśli do usługi Cyber Protection dodano wiele organizacji Hosted Exchange, kliknij **Organizacja usługi Hosted Exchange**, aby wyświetlić, zmienić lub określić organizację docelową.
   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
10. W polu **Odzyskaj do skrzynki pocztowej** wyświetl, zmień lub określ docelową skrzynkę pocztową.
    Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelową skrzynkę pocztową.
11. [Tylko w przypadku odzyskiwania do skrzynki pocztowej użytkownika lub współdzielonej] W sekcji **Ścieżka** wyświetl lub zmień folder docelowy w docelowej skrzynce pocztowej. Domyślnie wybrany jest folder **Odzyskane elementy**.
    Elementy skrzynki pocztowej grupy są zawsze odzyskiwane do folderu **skrzynka odbiorcza**.
12. Kliknij **Rozpocznij odzyskiwanie**.
13. Wybierz jedną z następujących opcji zastępowania:
    - **Zastąp istniejące elementy**
    - **Nie zastępuj istniejących elementów**
14. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Ochrona danych Microsoft 365

Dlaczego warto tworzyć kopie zapasowe danych Microsoft 365?

Choć Microsoft 365 jest pakietem usług chmurowych, regularnie tworzone kopie zapasowe stanowią dodatkową warstwę ochrony przed błędami użytkowników oraz celowo złośliwymi działaniami. Usunięte elementy można odzyskać z kopii zapasowej nawet po upłynięciu okresu ich przechowywania w usłudze Microsoft 365. Można też przechowywać lokalną kopię skrzynek pocztowych programu Exchange Online, jeśli wymaga tego obowiązek zachowania zgodności ze stosownymi przepisami.

Dane zapisywane w kopii zapasowej są automatycznie kompresowane i zajmują mniej miejsca w lokalizacji kopii zapasowych niż w pierwotnej lokalizacji. Poziom kompresji w przypadku kopii zapasowych z chmury do chmury jest stały i odpowiada poziomowi kompresji **Normalny** stosowanemu w przypadku innych kopii zapasowych. Dodatkowe informacje na temat tych poziomów można znaleźć w sekcji "Stopień kompresji" (s. 492).

Agent w chmurze i agent lokalny

Na potrzeby obciążeń Microsoft 365 dostępne są dwa agenty:

© Acronis International GmbH, 2003-2024

- Agent w chmurze

  Agent w chmurze zapewnia rozszerzone funkcje tworzenia kopii zapasowych, która są dostępne bezpośrednio w konsoli Cyber Protect. Nie jest wymagana żadna instalacja. Aby uzyskać więcej informacji, zobacz "Przy użyciu chmurowego agenta dla usługi Microsoft 365" (s. 651).
- Agent lokalny

  Agent lokalny obsługuje jedynie tworzenie kopii zapasowych skrzynek pocztowych programu Exchange Online. Agent ten musi być zainstalowany na podłączonym do Internetu komputerze z systemem Windows. Aby uzyskać więcej informacji, zobacz "Korzystanie z zainstalowanego lokalnie agenta dla Office 365" (s. 647).

Usługa Azure Information Protection (AIP) jest obsługiwana w przypadku obu agentów.

Uwaga
W przypadku dzierżawców w trybie zgodności jest dostępny tylko agent lokalny. Dzierżawcy ci mogą tworzyć kopie zapasowe tylko skrzynek pocztowych Microsoft 365. Nie mogą korzystać z rozszerzonych funkcji udostępnianych przez agenta w chmurze.

W poniższej tabeli zestawiono funkcje tych agentów.

	Agent lokalny	Agent w chmurze
Elementy danych, które można uwzględniać w kopiach zapasowych	**Exchange Online:** skrzynki pocztowe użytkowników i skrzynki udostępnione (w tym skrzynki pocztowe użytkowników korzystających z planu Kiosk oraz skrzynki pocztowe zabezpieczone do celów postępowania sądowego)	• **Exchange Online**: ◦ skrzynki pocztowe użytkowników i skrzynki udostępnione (w tym skrzynki pocztowe użytkowników korzystających z planu Kiosk oraz skrzynki pocztowe zabezpieczone do celów postępowania sądowego) ◦ skrzynki pocztowe grup ◦ foldery publiczne • **OneDrive**: pliki i foldery użytkowników • **SharePoint Online**: ◦ klasyczne zbiory witryn ◦ witryny grup (zespołów) ◦ witryny do komunikacji ◦ pojedyncze elementy danych • **Microsoft 365 Teams**: ◦ całe zespoły ◦ kanały zespołów ◦ pliki z kanałów

© Acronis International GmbH, 2003-2024

	Agent lokalny	Agent w chmurze
		◦ skrzynki pocztowe zespołów ◦ pliki i wiadomości e-mail ze skrzynek pocztowych zespołów ◦ spotkania ◦ witryny zespołów • **Notesy aplikacji OneNote**: w ramach kopii zapasowych aplikacji OneDrive, SharePoint Online i Microsoft 365 Teams
Kopie zapasowe archiwalnych skrzynek pocztowych (**archiwum zbiorcze**)	Nie	Tak
Harmonogram tworzenia kopii zapasowych	Zdefiniowany przez użytkownika	Do sześciu razy dziennie*
Lokalizacje kopii zapasowych	Chmura, folder lokalny, folder sieciowy	Tylko magazyn chmurowy (w tym pamięć masowa hostowana przez partnera)
Automatyczna ochrona nowych użytkowników, grup, witryn i zespołów w usłudze Microsoft 365	Nie	Tak, przez zastosowanie planu ochrony do grup **Wszyscy użytkownicy**, **Wszystkie grupy**, **Wszystkie witryny** i **Wszystkie zespoły**
Ochrona więcej niż jednej organizacji Microsoft 365	Nie	Tak
Granularne odzyskiwanie wybranych elementów	Tak	Tak
Odzyskiwanie do innego użytkownika w ramach jednej organizacji	Tak	Tak
Odzyskiwanie do innej organizacji	Nie	Tak
Odzyskiwanie na lokalny serwer Microsoft Exchange Server	Nie	Nie
Maksymalna liczba elementów, które można uwzględniać w kopiach	W przypadku tworzenie kopii zapasowej w chmurze: 5000 skrzynek pocztowych na firmę	10 000 chronionych elementów (skrzynki pocztowe, konta OneDrive lub witryny) na firmę**

© Acronis International GmbH, 2003-2024

	Agent lokalny	Agent w chmurze
zapasowych bez spadku wydajności	W przypadku tworzenia kopii zapasowych w innych miejscach docelowych: 2000 skrzynek pocztowych na plan ochrony (brak ograniczenia liczby skrzynek pocztowych na firmę)	
Maksymalna liczba ręcznie wykonywanych operacji tworzenia kopii zapasowej	Nie	10 ręcznie wykonywanych operacji tworzenia kopii zapasowej w ciągu godziny
Maksymalna liczba jednoczesnych operacji odzyskiwania	Nie	10 operacji, w tym operacje odzyskiwania dotyczące środowiska Google Workspace

* Domyślnie jest ustawiona opcja **Raz dziennie**. Pakiet Zaawansowane tworzenie kopii zapasowych umożliwia zaplanowanie do sześciu operacji tworzenia kopii zapasowych dziennie. Operacje tworzenia kopii zapasowych są uruchamiane w przybliżonych odstępach, które zależą od bieżącego obciążenia agenta w chmurze, obsługującego wielu klientów w centrum danych. Zapewnia to równomierne obciążenie w ciągu dnia i jednakową jakość obsługi wszystkich klientów.

Uwaga
Realizacja harmonogramu ochrony zależy od działania usług innych firm, na przykład dostępności serwerów Microsoft 365, ustawień ograniczania przepustowości na serwerach firmy Microsoft i innych. Zobacz też https://docs.microsoft.com/en-us/graph/throttling.

** Zalecamy etapowe tworzenie kopii zapasowych chronionych elementów w następującej kolejności:

1. Skrzynki pocztowe.
2. Po utworzeniu kopii zapasowej wszystkich skrzynek pocztowych przejdź do danych magazynu OneDrive.
3. Po utworzeniu kopii zapasowej danych magazynu OneDrive przejdź do witryn SharePoint Online.

Utworzenie pierwszej pełnej kopii zapasowej może potrwać kilka dni, w zależności od liczby i rozmiarów chronionych elementów.

Wymagane prawa użytkownika

W programie Cyber Protection

Agent lokalny musi być zarejestrowany na koncie administratora firmy i używany na poziomie dzierżawcy-klienta. Administratorzy firm działający na poziomie jednostek, administratorzy jednostek i użytkownicy nie mogą tworzyć kopii zapasowych ani odzyskiwać danych Microsoft 365.

© Acronis International GmbH, 2003-2024

Agenta w chmurze można używać zarówno na poziomie dzierżawcy-klienta, jak i na poziomie jednostki. Dodatkowe informacje na temat tych poziomów i ich administratorów można znaleźć w sekcji "Administrowanie organizacjami Microsoft 365 dodanymi na różnych poziomach" (s. 652).

W usłudze Microsoft 365

Twoje konto musi mieć przypisaną rolę administratora globalnego w usłudze Microsoft 365.

Aby można było wykryć foldery publiczne z usługi Microsoft 365, utworzyć ich kopię zapasową i je odzyskać, co najmniej jedno z kont administratora usługi Microsoft 365 musi mieć skrzynkę pocztową oraz prawa do odczytu/zapisu folderów publicznych, które mają zostać uwzględnione w kopii zapasowej.

- Agent lokalny zaloguje się do usługi Microsoft 365 przy użyciu tego konta. Aby umożliwić agentowi dostęp do zawartości wszystkich skrzynek pocztowych, kontu temu zostanie przypisana rola zarządzania **ApplicationImpersonation**. Jeśli zmienisz hasło do konta, zaktualizuj je w konsoli Cyber Protect zgodnie z opisem podanym w sekcji "Zmienianie poświadczeń dostępu do usługi Microsoft 365" (s. 649).
- Agent chmurowy nie loguje się do usługi Microsoft 365. Aby nadać agentowi w chmurze uprawnienia wymagane do jego działania, należy raz się zalogować do usługi Microsoft 365 jako administrator globalny.

  Wymagane są następujące uprawnienia w usłudze Microsoft 365:
  - Logowanie się i odczyt profilów użytkowników
  - Odczyt i zapis plików we wszystkich zbiorach witryn
  - Odczyt i zapis pełnych profilów wszystkich użytkowników
  - Odczyt i zapis wszystkich grup
  - Odczyt danych katalogu
  - Odczyt wszystkich komunikatów kanału
  - Odczyt i zapis wszystkich zarządzanych metadanych
  - Odczyt i zapis elementów oraz list we wszystkich zbiorach witryn
  - Pełna kontrola nad wszystkimi zbiorami witryn
  - Odczyt i zapis elementów we wszystkich zbiorach witryn
  - Możliwość korzystania z Usług sieci Web programu Exchange z pełnym dostępem do wszystkich skrzynek pocztowych
- Agent w chmurze nie przechowuje poświadczeń Twojego konta ani nie używa ich do tworzenia kopii zapasowych bądź odzyskiwania. Zmiana poświadczeń, wyłączenie konta lub usunięcie konta nie ma wpływu na działanie agenta w chmurze.

Ograniczenia

- Za pomocą agenta lokalnego można chronić do 5000 maszyn. Za pomocą agenta w chmurze można chronić do 50 000 maszyn.

© Acronis International GmbH, 2003-2024

- Wszyscy użytkownicy mający skrzynkę pocztową lub dysk OneDrive są widoczni na liście w konsoli Cyber Protect, w tym użytkownicy niemający licencji na usługi Microsoft 365 oraz użytkownicy, którzy mają zablokowaną możliwość logowania się do usług Microsoft 365.
- Kopia zapasowa skrzynek pocztowych obejmuje tylko foldery widoczne dla użytkowników. Folder **Elementy odzyskiwalne** i jego podfoldery (**Usunięcia**, **Wersje**, **Oczyszczone**, **Audyty**, **DiscoveryHold**, **Rejestrowanie kalendarza**] nie są uwzględniane w kopii zapasowej.
- Automatyczne tworzenie użytkowników, folderów publicznych, grup i witryn podczas odzyskiwania nie jest możliwe. Na przykład jeśli chcesz odzyskać usuniętą witrynę SharePoint Online, najpierw utwórz ręcznie nową witrynę, a następnie ustaw ją jako witrynę docelową podczas odzyskiwania.
- Nie można równolegle odzyskiwać elementów z różnych punktów odzyskiwania, nawet jeśli da się wybrać takie elementy z wyników wyszukiwania.
- Podczas tworzenia kopii zapasowej wszelkie etykiety wrażliwości zastosowane do zawartości zostają zachowane. W związku z tym ewentualna wrażliwa zawartość nie będzie wyświetlana, jeśli zostanie odzyskana w lokalizacji innej niż pierwotna, a użytkownik ma inne uprawnienia dostępu.
- Do danego obciążenia nie można zastosować więcej niż jednego indywidualnego planu tworzenia kopii zapasowych.
- Jeśli do tego samego obciążenia zastosowano indywidualny plan tworzenia kopii zapasowych i grupowy plan tworzenia kopii zapasowych, ustawienia planu indywidualnego mają pierwszeństwo.

Raport o licencjonowaniu stanowisk Microsoft 365

Administratorzy firmy mogą pobrać raport o chronionych stanowiskach Microsoft 365 i ich licencjonowaniu. Raport jest dostępny w formacie CSV i zawiera informacje o statusie licencjonowania danego stanowiska oraz przyczynie wykorzystania licencji. Raport zawiera też nazwę chronionego stanowiska, powiązany z nim adres e-mail, grupę, organizację Microsoft 365, nazwę i typ chronionego obciążenia.

Raport ten jest dostępny tylko dla dzierżawców, w ramach których zarejestrowano organizację Microsoft 365.

Aby pobrać raport o licencjonowaniu stanowisk Microsoft 365

1. Zaloguj się do konsoli Cyber Protect jako administrator firmy.
2. Kliknij ikonę konta w prawym górnym rogu.
3. Kliknij **Raport o licencjonowaniu stanowisk Microsoft 365**.

Prowadzenie dziennika

Niektóre czynności dotyczące zasobów międzychmurowych, takie jak przeglądanie zawartości wiadomości e-mail w kopiach zapasowych, pobieranie załączników lub plików, odzyskiwanie wiadomości e-mail do skrzynek pocztowych innych niż pierwotne lub wysyłanie zasobów jako

© Acronis International GmbH, 2003-2024

wiadomości e-mail, mogą naruszać prywatność użytkowników. Czynności te są rejestrowane w sekcji **Monitorowanie** > **Dziennik inspekcji** w portalu zarządzania.

Korzystanie z zainstalowanego lokalnie agenta dla Office 365

Dodawanie organizacji Microsoft 365

Aby dodać organizację Microsoft 365

1. Zaloguj się do konsoli Cyber Protect jako administrator firmy.
2. Kliknij ikonę konta w prawym górnym rogu, a następnie kliknij **Do pobrania** > **Agent dla usługi Office 365**.
3. Pobierz agenta i zainstaluj go na podłączonym do Internetu komputerze z systemem Windows.
4. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft Office 365 (agent lokalny)**.
5. W otwartym oknie wprowadź identyfikator i klucz tajny aplikacji oraz identyfikator dzierżawcy Microsoft 365. Dodatkowe informacje o tym, jak je znaleźć, zawiera sekcja "Uzyskiwanie identyfikatora i klucza tajnego aplikacji" (s. 647).
6. Kliknij **OK**.

W wyniku tych działań elementy danych organizacji pojawią się w konsoli Cyber Protect — na karcie **Microsoft Office 365 (agent lokalny)**.

Ważne
W organizacji (grupie firmy) musi się znajdować tylko jeden zainstalowany lokalnie agent dla usługi Office 365.

Uzyskiwanie identyfikatora i klucza tajnego aplikacji

Aby korzystać z nowoczesnej technologii uwierzytelniania w usłudze Office 365, trzeba utworzyć aplikację niestandardową centrum administracyjnym Entra i nadać jej określone uprawnienia do interfejsów API. W ten sposób uzyskasz **identyfikator aplikacji**, **klucz tajny aplikacji** oraz **identyfikator katalogu (dzierżawcy)**, które trzeba wprowadzić w konsoli Cyber Protect.

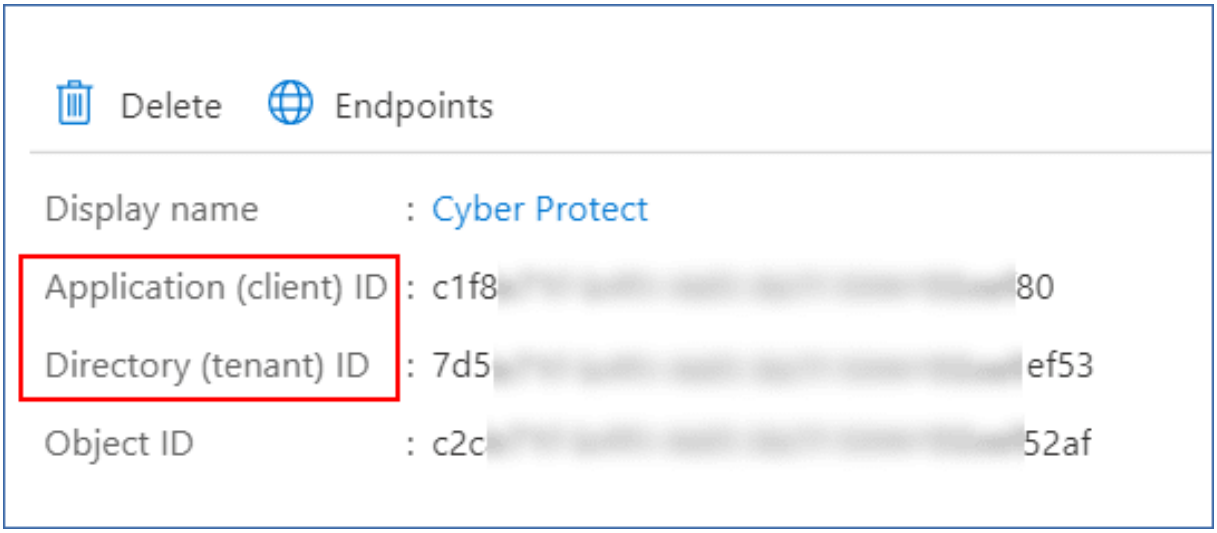
Uwaga
Dopilnuj, aby na komputerze z zainstalowanym agentem dla usługi Office 365 był dozwolony dostęp do adresu graph.microsoft.com przez port 443.

Aby utworzyć aplikację w centrum administracyjnym Entra

1. Zaloguj się do centrum administracyjnego Entra jako administrator.
2. Przejdź do sekcji **Azure Active Directory** > **Rejestracje aplikacji** i kliknij **Nowa rejestracja**.
3. Określ nazwę aplikacji niestandardowej, na przykład Cyber Protection.
4. W polu **Obsługiwane typy kont** zaznacz **Tylko konta w tym katalogu organizacyjnym**.
5. Kliknij **Zarejestruj**.

© Acronis International GmbH, 2003-2024

Aplikacja została utworzona. W centrum administracyjnym Entra przejdź do strony **Przegląd** aplikacji i sprawdź jej identyfikator (klienta) oraz identyfikator katalogu (dzierżawcy).



Więcej informacji na temat tworzenia aplikacji w centrum administracyjnym Entra można znaleźć w dokumentacji firmy Microsoft.

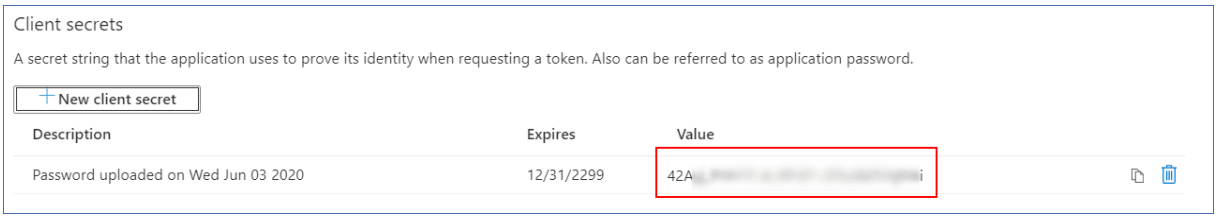
Aby przyznaj aplikacji niezbędne uprawnienia do interfejsów API

1. W centrum administracyjnym Entra przejdź do sekcji **Uprawnienia interfejsu API** aplikacji i kliknij **Dodaj uprawnienie**.
2. Wybierz kartę **Interfejsy API, z których korzysta moja organizacja** i wyszukaj **Office 365 Exchange Online**.
3. Kliknij **Office 365 Exchange Online**, a następnie kliknij **Uprawnienia aplikacji**.
4. Zaznacz pole wyboru **full_access_as_app** i kliknij **Dodaj uprawnienia**.
5. W polu **Uprawnienia interfejsu API** kliknij **Dodaj uprawnienie**.
6. Wybierz **Microsoft Graph**.
7. Wybierz **Uprawnienia aplikacji**.
8. Rozwiń kartę **Katalog** i zaznacz pole wyboru **Directory.Read.All**. Kliknij **Dodaj uprawnienia**.
9. Sprawdź wszystkie uprawnienia i kliknij **Przyznaj zgodę administratora na rejestrację aplikacji <nazwa aplikacji>**.
10. Potwierdź wybór, klikając **Tak**.

Aby utworzyć klucz tajny aplikacji

1. W centrum administracyjnym Entra przejdź do sekcji **Certyfikaty i klucze tajne** > **Nowy klucz tajny klienta**.
2. W nowo otwartym oknie dialogowym zaznacz Wygasa: **Nigdy** i kliknij **Dodaj**.
3. Sprawdź klucz tajny aplikacji w polu **Wartość** i koniecznie go zapamiętaj.

© Acronis International GmbH, 2003-2024



Więcej informacji na temat klucza tajnego aplikacji można znaleźć w dokumentacji firmy Microsoft.

Zmienianie poświadczeń dostępu do usługi Microsoft 365

Poświadczenia dostępu do usługi Microsoft 365 można zmienić bez ponownego instalowania agenta.

Aby zmienić poświadczenia dostępu do usługi Microsoft 365

1. Kliknij **Urządzenia** > **Microsoft Office 365 (agent lokalny)**.
2. Wybierz organizację Microsoft 365.
3. Kliknij **Określ poświadczenia**.
4. Wprowadź identyfikator i klucz tajny aplikacji oraz identyfikator dzierżawcy Microsoft 365. Dodatkowe informacje o tym, jak je znaleźć, zawiera sekcja "Uzyskiwanie identyfikatora i klucza tajnego aplikacji" (s. 647).
5. Kliknij **OK**.

Ochrona skrzynek pocztowych programu Exchange Online

Jakie elementy można uwzględnić w kopii zapasowej?

W kopii zapasowej można uwzględnić skrzynki pocztowe użytkowników oraz skrzynki współdzielone. Nie można tworzyć kopii zapasowych grupowych ani archiwalnych skrzynek pocztowych (**archiwum zbiorczego**).

Jakie elementy można odzyskać?

Z kopii zapasowej skrzynek pocztowych można odzyskać następujące elementy:

- Skrzynki pocztowe
- Foldery poczty e-mail
- Wiadomości e-mail
- Zdarzenia kalendarza
- Zadania
- Kontakty
- Wpisy dziennika
- Notatki

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

© Acronis International GmbH, 2003-2024

W przypadku odzyskiwania skrzynki pocztowej do już istniejącej skrzynki dostępne w niej elementy o takich samych identyfikatorach zostaną zastąpione.

Odzyskiwanie elementów skrzynki pocztowej nie powoduje zastępowania żadnych danych. Zamiast tego w folderze docelowym zostanie odtworzona pełna ścieżka elementu skrzynki pocztowej.

Wybieranie skrzynek pocztowych Microsoft 365

Wybierz skrzynki pocztowe zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać skrzynki pocztowe

1. Kliknij **Microsoft Office 365 (agent lokalny)**.
2. Wybierz skrzynki pocztowe, które chcesz uwzględnić w kopii zapasowej.
3. Kliknij **Kopia zapasowa**.

Odzyskiwanie skrzynek pocztowych i elementów skrzynek pocztowych

Odzyskiwanie skrzynek pocztowych

1. Kliknij **Microsoft Office 365 (agent lokalny)**.
2. Wybierz skrzynkę pocztową do odzyskania, a następnie kliknij **Odzyskiwanie**.
   Skrzynki pocztowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
   Jeśli skrzynka pocztowa została usunięta, zaznacz ją na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
3. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Skrzynka pocztowa**.
5. W polu **Docelowa skrzynka pocztowa** wyświetl, zmień lub określ docelową skrzynkę pocztową.
   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli tej skrzynki pocztowej już nie ma, trzeba określić docelową skrzynkę pocztową.
6. Kliknij **Rozpocznij odzyskiwanie**.

Odzyskiwanie elementów skrzynki pocztowej

1. Kliknij **Microsoft Office 365 (agent lokalny)**.
2. Wybierz skrzynkę pocztową, która pierwotnie zawierała elementy do odzyskania, a następnie kliknij **Odzyskiwanie**.
   Skrzynki pocztowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
   Jeśli skrzynka pocztowa została usunięta, zaznacz ją na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
3. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
5. Wybierz elementy, które chcesz odzyskać.

© Acronis International GmbH, 2003-2024

Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.

- Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata, nazwy załącznika i daty.
- Zdarzenia: wyszukiwanie według tematu i daty.
- Zadania: wyszukiwanie według tematu i daty.
- Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.

Po zaznaczeniu wiadomości e-mail możesz kliknąć **Pokaż zawartość**, aby wyświetlić jej zawartość, w tym załączniki.

Uwaga
Kliknij nazwę załączonego pliku, aby go pobrać.

Po zaznaczeniu wiadomości e-mail możesz kliknąć **Wyślij jako wiadomość e-mail**, aby wysłać wiadomość na jakiś adres e-mail. Wiadomość zostanie wysłana z adresu email konta administratora.

Aby mieć możliwość wybrania folderów, kliknij ikonę „Odzyskaj foldery”:

6. Kliknij **Odzyskaj**.
7. W polu **Docelowa skrzynka pocztowa** wyświetl, zmień lub określ docelową skrzynkę pocztową.
   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli tej skrzynki pocztowej już nie ma, trzeba określić docelową skrzynkę pocztową.
8. Kliknij **Rozpocznij odzyskiwanie**.
9. Potwierdź decyzję.

Elementy skrzynki pocztowej są zawsze odzyskiwane do folderu **Odzyskane elementy** docelowej skrzynki pocztowej.

Przy użyciu chmurowego agenta dla usługi Microsoft 365

Dodawanie organizacji Microsoft 365

Administrator może dodać do dzierżawcy-klienta lub jednostki jedną lub więcej organizacji Microsoft 365.

Administratorzy firmy dodają organizacje do dzierżawców-klientów. Administratorzy jednostek i administratorzy klientów działający na poziomie jednostki dodają organizacje do jednostek.

Aby dodać organizację Microsoft 365

1. W zależności od tego, gdzie ma zostać dodana organizacja, zaloguj się do konsoli Cyber Protect jako administrator firmy lub administrator jednostki.
2. [W przypadku administratora firmy działającego na poziomie jednostki] W portalu zarządzania przejdź do odpowiedniej jednostki.
3. Kliknij **Urządzenia** > **Dodaj** > **Microsoft 365 Business**.
   Oprogramowanie przekieruje Cię na stronę logowania do usługi Microsoft 365.

© Acronis International GmbH, 2003-2024

4. Zaloguj się przy użyciu poświadczeń administratora globalnego usługi Microsoft 365.
   W usłudze Microsoft 365 wyświetlana jest lista uprawnień niezbędnych do tworzenia kopii zapasowych i odzyskiwania danych organizacji.
5. Potwierdź przyznanie uprawnień usłudze Cyber Protection.

W wyniku tych działań organizacja Microsoft 365 pojawi się na karcie **Urządzenia** w konsoli Cyber Protect.

Przydatne porady

- Agent w chmurze synchronizuje się z usługą Microsoft 365 co 24 godziny, zaczynając od chwili dodania organizacji do usługi Cyber Protection. Jeśli dodasz lub usuniesz użytkownika, grupę czy witrynę, zmiany nie będą od razu widoczne w konsoli Cyber Protect. Aby niezwłocznie zsynchronizować zmianę, wybierz organizację na stronie **Microsoft 365**, a następnie kliknij **Odśwież**.
  Dodatkowe informacje na temat synchronizowania zasobów organizacji Microsoft 365 i konsoli Cyber Protect można znaleźć w sekcji "Wykrywanie zasobów z usługi Microsoft 365" (s. 654).
- Jeśli plan ochrony został zastosowany do grupy **Wszyscy użytkownicy**, **Wszystkie grupy** lub **Wszystkie lokalizacje**, nowo dodane elementy zostaną uwzględnione w kopii zapasowej dopiero po synchronizacji.
- Zgodnie z zasadami firmy Microsoft po usunięciu użytkownika, grupy lub lokalizacji z graficznego interfejsu użytkownika pakietu Microsoft 365 jeszcze przez kilka dni można uzyskać do nich dostęp za pośrednictwem interfejsu API. W tym okresie usunięty element jest nieaktywny (wyszarzony) w konsoli Cyber Protect i nie jest uwzględniany w kopiach zapasowych. Gdy usunięty element przestanie być dostępny za pośrednictwem interfejsu API, przestanie też być widoczny w konsoli Cyber Protect. Jego kopie zapasowe (jeśli jakieś istnieją) można znaleźć w obszarze **Magazyn kopii zapasowych** > **Kopie zapasowe aplikacji w chmurze**.

Administrowanie organizacjami Microsoft 365 dodanymi na różnych poziomach

Administratorzy firmy mają pełny dostęp do organizacji Microsoft 365 dodanych na poziomie dzierżawcy-klienta.

Administratorzy firmy mają ograniczony dostęp do organizacji dodanych na poziomie jednostki. W przypadku tych organizacji, wyświetlanych z nazwą jednostki w nawiasach, administratorzy firmy mogą wykonywać następujące operacje:

- Odzyskiwanie danych z kopii zapasowych.
  Administratorzy firmy mogą odzyskiwać dane do wszystkich organizacji w ramach dzierżawcy, niezależnie od poziomu, na którym te organizacje zostały dodane.
- Przeglądanie kopii zapasowych i punktów odzyskiwania w kopiach zapasowych.
- Usuwanie kopii zapasowych i punktów odzyskiwania z kopii zapasowych.
- Wyświetlanie alertów i działań.

© Acronis International GmbH, 2003-2024

Administratorzy firmy działający na poziomie dzierżawcy-klienta nie mogą wykonywać następujących operacji:

- Dodawanie organizacji Microsoft 365 do jednostek.
- Usuwanie organizacji Microsoft 365 z jednostek.
- Synchronizowanie organizacji Microsoft 365 dodanych do jednostki.
- Wyświetlanie, tworzenie, edytowanie, usuwanie, stosowanie, uruchamianie lub odwoływanie planów ochrony w odniesieniu do elementów danych w organizacjach Microsoft 365 dodanych do jednostki.

Administratorzy jednostki i administratorzy firmy działający na poziomie jednostki mają pełny dostęp do organizacji dodanych do jednostki. Nie mają jednak dostępu do żadnych zasobów w obszarze nadrzędnego dzierżawcy-klienta, w tym do planów ochrony, które zostały utworzone w jego ramach.

Usuwanie organizacji Microsoft 365

Usunięcie organizacji Microsoft 365 nie ma wpływu na istniejące już kopie zapasowe danych tej organizacji. Jeśli te kopie zapasowe nie są już potrzebne, usuń najpierw je, a następnie organizację Microsoft 365. Jeśli tego nie zrobisz, te kopie zapasowe będą nadal zajmować miejsce w chmurze, za które mogą być naliczane opłaty.

Dodatkowe informacje na temat usuwania kopii zapasowych można znaleźć w sekcji "Aby usunąć kopie zapasowe lub archiwa kopii zapasowych" (s. 572).

Aby usunąć organizację Microsoft 365

1. W zależności od tego, gdzie została dodana organizacja, zaloguj się do konsoli Cyber Protect jako administrator firmy lub administrator jednostki.
2. [W przypadku administratora firmy działającego na poziomie jednostki] W portalu zarządzania przejdź do odpowiedniej jednostki.
3. Przejdź do sekcji **Urządzenia** > **Microsoft 365**.
4. Wybierz organizację i kliknij **Usuń grupę**.

W wyniku tego plany tworzenia kopii zapasowych zastosowane do tej grupy zostaną odwołane.

Należy jednak jeszcze ręcznie cofnąć uprawnienia dostępu aplikacji Usługa kopii zapasowych do danych organizacji Microsoft 365.

Aby cofnąć prawa dostępu

1. Zaloguj się do usługi Microsoft 365 jako administrator globalny.
2. Przejdź do sekcji **Centrum administracyjne** > **Azure Active Directory** > **Aplikacje dla przedsiębiorstw** > **Wszystkie aplikacje**.
3. Wybierz aplikację **Usługa kopii zapasowych** i przejdź na jej poziom.

© Acronis International GmbH, 2003-2024

4. Wybierz kartę **Właściwości** i na panelu czynności kliknij **Usuń**.
5. Potwierdź operację usunięcia.

W wyniku tego prawa dostępu do danych organizacji Microsoft 365 zostaną cofnięte z aplikacji Usługa kopii zapasowych.

Wykrywanie zasobów z usługi Microsoft 365

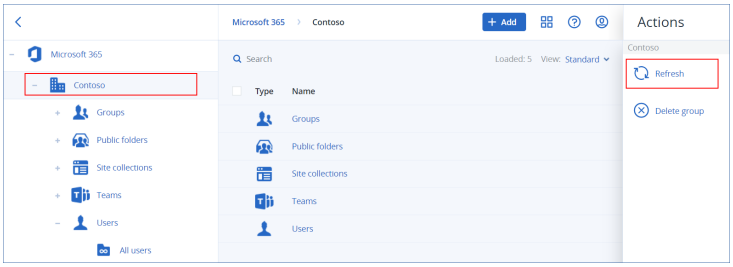
W przypadku dodania organizacji Microsoft 365 do rozwiązania Cyber Protection zasoby z tej organizacji, na przykład skrzynki pocztowe, magazyny usługi OneDrive, dane Microsoft Teams i witryny SharePoint, są synchronizowane z konsolą Cyber Protect. Operacja ta jest nazywana wykrywaniem i jest rejestrowana w sekcji **Monitorowanie** > **Działania**.

Po zakończeniu operacji wykrywania zasoby z organizacji Microsoft 365 będą widoczne na karcie **Urządzenia** > **Microsoft 365** w konsoli Cyber Protect i będzie można stosować do nich plany tworzenia kopii zapasowych.

Operacja wykrywania jest wykonywana automatycznie raz dziennie, aby zapewnić aktualność listy zasobów w konsoli Cyber Protect. Listę tę można też synchronizować na żądanie przez ręczne uruchomienie operacji wykrywania.

Aby ręcznie uruchomić operację wykrywania

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft 365**.
2. Zaznacz organizację Microsoft 365, a następnie w panelu **Czynności** kliknij **Odśwież**.



Uwaga
Operację wykrywania można uruchomić ręcznie do 10 razy na godzinę. Po osiągnięciu tej liczby ustawienie limitu dozwolonych uruchomień zostaje ograniczone do jednego razu na godzinę, a następnie co godzinę udostępniana jest dodatkowa operacja, aż do ponownego osiągnięcia limitu 10 operacji na godzinę.

Ustawianie częstotliwości tworzenia kopii zapasowych danych pakietu Microsoft 365

Domyślnie kopie zapasowe danych pakietu Microsoft 365 są tworzone raz dziennie i nie ma dodatkowych opcji planowania.

© Acronis International GmbH, 2003-2024

Jeśli w ramach dzierżawcy jest włączony pakiet Zaawansowane tworzenie kopii zapasowych, można skonfigurować częstsze tworzenie kopii zapasowych. Można wybrać liczbę kopii zapasowych dziennie, ale nie można skonfigurować godziny rozpoczęcia operacji tworzenia kopii zapasowej. Operacje tworzenia kopii zapasowych są uruchamiane automatycznie w przybliżonych odstępach, które zależą od bieżącego obciążenia agenta w chmurze, obsługującego wielu klientów w centrum danych. Zapewnia to równomierne obciążenie w ciągu dnia i jednakową jakość obsługi wszystkich klientów.

Dostępne są następujące opcje.

Opcje planowania	Przybliżony odstęp między operacjami tworzenia kopii zapasowych
Raz dziennie	24 godz.
2 razy dziennie (domyślnie)	12 godzin
3 razy dziennie	8 godzin
6 razy dziennie	4 godziny

Uwaga
W zależności od obciążenia agenta w chmurze i ewentualnego ograniczenia po stronie Microsoft 365 tworzenie kopii zapasowej może się rozpocząć później niż zaplanowano lub potrwać dłużej. Jeśli tworzenie kopii zapasowej trwa dłużej niż średni odstęp czasowy między dwiema operacjami tworzenia kopii zapasowych, następna kopia zapasowa zostanie przełożona, co może skutkować mniejszą liczbą kopii zapasowych dziennie niż wybrano. Na przykład, mogą zostać utworzone tylko dwie kopie zapasowe dziennie — nawet jeśli wybrano sześć kopii dziennie.

Kopie zapasowe skrzynek pocztowych grup mogą być tworzone tylko raz dziennie.

Ochrona danych programu Exchange Online

Jakie elementy można uwzględnić w kopii zapasowej?

W kopii zapasowej można uwzględnić skrzynki pocztowe użytkowników i grup oraz skrzynki współdzielone. Opcjonalnie można wybrać tworzenie kopii zapasowej archiwalnych skrzynek pocztowych online (**archiwum zbiorczego**) dla wybranych skrzynek.

Od wersji 8.0 usługi Cyber Protection dostępna jest możliwość tworzenia kopii zapasowych folderów publicznych. Jeśli organizacja została dodana do usługi Cyber Protection przed wydaniem wersji 8.0, trzeba ją ponownie dodać, aby móc skorzystać z tej funkcji. Nie usuwaj organizacji — wystarczy, że ponownie wykonasz czynności opisane w sekcji "Dodawanie organizacji Microsoft 365" (s. 651). W wyniku tego usługa Cyber Protection uzyska uprawnienie do korzystania z odpowiedniego interfejsu API.

Jakie elementy można odzyskać?

Z kopii zapasowej skrzynek pocztowych można odzyskać następujące elementy:

© Acronis International GmbH, 2003-2024

- Skrzynki pocztowe
- Foldery poczty e-mail
- Wiadomości e-mail
- Zdarzenia kalendarza
- Zadania
- Kontakty
- Wpisy dziennika
- Notatki

Z kopii zapasowej folderu publicznego można odzyskać następujące elementy:

- Podfoldery
- Posty
- Wiadomości e-mail

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

Odzyskując skrzynki pocztowe, elementy skrzynek pocztowych, foldery publiczne i elementy folderów publicznych, można wybrać, czy elementy w lokalizacji docelowej mają zostać zastąpione.

Wybór skrzynek pocztowych

Wybierz skrzynki pocztowe zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać skrzynki pocztowe programu Exchange Online

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę organizację, w której przypadku chcesz utworzyć kopię zapasową danych użytkowników. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby tworzyć kopie zapasowe wszystkich skrzynek pocztowych użytkowników i wszystkich skrzynek współdzielonych (w tym skrzynek, które zostaną utworzone w przyszłości), rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby tworzyć kopie zapasowe wybranych skrzynek pocztowych użytkowników lub skrzynek współdzielonych, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wybierz użytkowników, których skrzynki pocztowe chcesz uwzględniać w kopiach zapasowych, i kliknij **Kopia zapasowa**.
   - Aby tworzyć kopie zapasowe skrzynek pocztowych wszystkich grup (w tym skrzynek, które zostaną utworzone w przyszłości), rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie kliknij **Kopia zapasowa grupy**.

© Acronis International GmbH, 2003-2024

- Aby tworzyć kopie zapasowe wybranych grupowych skrzynek pocztowych, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, następnie wskaż grupy, dla których chcesz wykonać kopię zapasową skrzynek pocztowych, po czym kliknij **Kopia zapasowa**.

  Uwaga
  Dostępny w chmurze agent dla usługi Microsoft 365 korzysta z konta, które ma odpowiednie prawa dostępu do skrzynki pocztowej grupy. Aby więc utworzyć kopię zapasową skrzynki pocztowej grupy, co najmniej jeden z właścicieli grupy musi być licencjonowanym użytkownikiem usługi Microsoft 365 i mieć skrzynkę pocztową. Jeśli grupa jest prywatna lub jej członkostwo jest ukryte, właściciel musi też być członkiem grupy.

4. W panelu planu ochrony:
   - Upewnij się, że w sekcji **Elementy uwzględniane w kopii zapasowej** jest zaznaczona pozycja **Skrzynki pocztowe Microsoft 365**.

     Jeśli niektórzy z indywidualnie wybranych użytkowników nie mają aplikacji Exchange w swoim planie usługi Microsoft 365, nie będzie można wybrać tej opcji.

     Jeśli niektórzy z użytkowników wybranych do kopii zapasowej grupy nie mają rozwiązania OneDrive w swoim planie usługi Microsoft 365, będzie można wybrać tę opcję, ale plan ochrony nie będzie do nich stosowany.
   - Jeśli nie chcesz tworzyć kopii zapasowych archiwalnych skrzynek pocztowych, wyłącz przełącznik **Archiwizuj skrzynkę pocztową**.

Wybieranie folderów publicznych

Wybierz foldery publiczne zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Uwaga
Foldery publiczne wykorzystują licencje z limitu kopii zapasowych stanowisk Microsoft 365.

Aby wybrać foldery publiczne programu Exchange Online

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, rozwiń tę organizację, której dane chcesz uwzględnić w kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Foldery publiczne** i wybierz **Wszystkie foldery publiczne**.
4. Wykonaj jedną z następujących czynności:
   - Aby tworzyć kopie zapasowe wszystkich folderów publicznych (w tym folderów publicznych, które zostaną utworzone w przyszłości), kliknij **Kopia zapasowa grupy**.
   - Aby utworzyć kopię zapasową wybranych folderów publicznych, wybierz foldery publiczne do uwzględnienia w kopii zapasowej i kliknij **Kopia zapasowa**.
5. Dopilnuj, aby w panelu planu ochrony w sekcji **Elementy uwzględniane w kopii zapasowej** była zaznaczona opcja **Skrzynki pocztowe Microsoft 365**.

© Acronis International GmbH, 2003-2024

Odzyskiwanie skrzynek pocztowych i elementów skrzynek pocztowych

Odzyskiwanie skrzynek pocztowych

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby odzyskać skrzynkę pocztową użytkownika, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż użytkownika, którego skrzynkę pocztową chcesz odzyskać, po czym kliknij **Odzyskiwanie**.
   - Aby odzyskać współdzieloną skrzynkę pocztową, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż skrzynkę współdzieloną, którą chcesz odzyskać, i kliknij **Odzyskiwanie**.
   - Aby odzyskać skrzynkę pocztową grupy, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie wskaż grupę, której skrzynkę pocztową chcesz odzyskać, po czym kliknij **Odzyskiwanie**.
   - Jeśli skrzynka pocztowa użytkownika, grupy lub współdzielona została usunięta, wybierz element w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

   Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

   Uwaga
   Aby wyświetlić wyłącznie punkty odzyskiwania zawierające skrzynki pocztowe, wybierz opcję **Skrzynki pocztowe** w sekcji **Filtruj według zawartości**.

5. Kliknij **Odzyskaj** > **Cała skrzynka pocztowa**.
6. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.
   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
7. W polu **Odzyskaj do skrzynki pocztowej** wyświetl, zmień lub określ docelową skrzynkę pocztową.
   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelową skrzynkę pocztową.
   Podczas odzyskiwania nie można utworzyć nowej docelowej skrzynki pocztowej. Aby odzyskać skrzynkę pocztową do nowej skrzynki pocztowej, trzeba najpierw utworzyć docelową skrzynkę pocztową w wybranej organizacji Microsoft 365, a następnie pozwolić agentowi w chmurze zsynchronizować zmianę. Agent w chmurze automatycznie synchronizuje się z usługą Microsoft

© Acronis International GmbH, 2003-2024

365 co 24 godziny. Aby niezwłocznie zsynchronizować zmianę, w konsoli Cyber Protect wybierz organizację na stronie **Microsoft 365**, a następnie kliknij **Odśwież**.

8. Kliknij **Rozpocznij odzyskiwanie**.
9. Wybierz jedną z następujących opcji zastępowania:
   - **Zastąp istniejące elementy**
   - **Nie zastępuj istniejących elementów**
10. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Odzyskiwanie elementów skrzynki pocztowej

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby odzyskać elementy ze skrzynki pocztowej użytkownika, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż użytkownika, którego skrzynka pocztowa pierwotnie zawierała elementy do odzyskania, po czym kliknij **Odzyskiwanie**.
   - Aby odzyskać elementy ze współdzielonej skrzynki pocztowej, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż skrzynkę współdzieloną pierwotnie zawierającą elementy, które chcesz odzyskać, i kliknij **Odzyskiwanie**.
   - Aby odzyskać elementy ze skrzynki pocztowej grupy, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie wskaż grupę, której skrzynka pocztowa pierwotnie zawierała elementy do odzyskania, po czym kliknij **Odzyskiwanie**.
   - Jeśli skrzynka pocztowa użytkownika, grupy lub współdzielona została usunięta, wybierz element w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

   Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

   Uwaga
   Aby wyświetlić wyłącznie punkty odzyskiwania zawierające skrzynki pocztowe, wybierz opcję **Skrzynki pocztowe** w sekcji **Filtruj według zawartości**.

5. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
6. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów.

   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.
   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata, nazwy załącznika i daty. Możesz wybrać datę początkową lub końcową (obie włącznie) albo obie te daty, aby wyszukiwać w zakresie czasu.

© Acronis International GmbH, 2003-2024

- Zdarzenia: wyszukiwanie według tematu i daty.
- Zadania: wyszukiwanie według tematu i daty.
- Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.

7. Wybierz elementy, które chcesz odzyskać. Aby mieć możliwość wybrania folderów, kliknij ikonę „Odzyskaj foldery”:

   Podczas odzyskiwania nie można utworzyć nowej docelowej skrzynki pocztowej. Aby odzyskać nowy element skrzynki pocztowej do nowej skrzynki pocztowej, trzeba najpierw utworzyć docelowy nowy element skrzynki pocztowej w organizacji Microsoft 365, a następnie pozwolić agentowi w chmurze zsynchronizować zmianę. Agent w chmurze automatycznie synchronizuje się z usługą Microsoft 365 co 24 godziny. Aby niezwłocznie zsynchronizować zmianę, w konsoli Cyber Protect wybierz organizację na stronie **Microsoft 365**, a następnie kliknij **Odśwież**.

   Możesz również wykonać dowolną z następujących czynności:
   - Po wybraniu elementu kliknij **Pokaż zawartość**, aby wyświetlić jego zawartość, łącznie z załącznikami. Kliknij nazwę załączonego pliku, aby go pobrać.
   - Po zaznaczeniu wiadomości e-mail lub elementu kalendarza możesz kliknąć **Wyślij jako wiadomość e-mail**, aby wysłać ten element na wskazany adres e-mail. Możesz wybrać nadawcę i napisać tekst, który zostanie dołączony do przekazywanego elementu.
   - Tylko w sytuacji, gdy kopia zapasowa nie jest zaszyfrowana, a w wynikach wyszukiwania wybrano jeden element: kliknij **Pokaż wersje**, aby wybrać wersję elementu do odzyskania. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.
8. Kliknij **Odzyskaj**.
9. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.

   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
10. W polu **Odzyskaj do skrzynki pocztowej** wyświetl, zmień lub określ docelową skrzynkę pocztową.

    Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelową skrzynkę pocztową.
11. [Tylko w przypadku odzyskiwania do skrzynki pocztowej użytkownika lub współdzielonej] W sekcji **Ścieżka** wyświetl lub zmień folder docelowy w docelowej skrzynce pocztowej. Domyślnie wybrany jest folder **Odzyskane elementy**.

    Elementy skrzynki pocztowej grupy są zawsze odzyskiwane do folderu **skrzynka odbiorcza**.
12. Kliknij **Rozpocznij odzyskiwanie**.
13. Wybierz jedną z następujących opcji zastępowania:
    - **Zastąp istniejące elementy**
    - **Nie zastępuj istniejących elementów**
14. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

© Acronis International GmbH, 2003-2024

Odzyskiwanie całych skrzynek pocztowych do plików danych PST

Uwaga
W ramach odzyskiwania do plików PST nie można przywrócić archiwum zbiorczego. Jeśli chcesz przywrócić archiwum zbiorcze wraz ze skrzynką pocztową, zobacz sekcję "Odzyskiwanie skrzynek pocztowych" (s. 658).

Aby odzyskać skrzynkę pocztową

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby odzyskać skrzynkę pocztową użytkownika do pliku danych PST, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, wskaż skrzynkę pocztową, którą chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
   - Aby odzyskać udostępnioną skrzynkę pocztową do pliku danych PST, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, wskaż skrzynkę pocztową, którą chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
   - Aby odzyskać skrzynkę pocztową grupy do pliku PST, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie wskaż grupę, której skrzynkę pocztową chcesz odzyskać, po czym kliknij **Odzyskiwanie**.

   Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.

   Jeśli plik danych programu Outlook ze skrzynką pocztową użytkownika, grupy lub udostępnioną została usunięta, wybierz element w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
4. Kliknij **Odzyskaj** > **Jako pliki PST**.
5. Ustaw hasło w celu zaszyfrowania archiwum z plikami PST.
   Hasło musi się składać z co najmniej 1 znaku.
6. Potwierdź hasło i kliknij **Gotowe**.
7. Wybrane elementy skrzynki pocztowej zostaną odzyskane jako pliki danych PST i zarchiwizowane w formacie ZIP. Plik PST może mieć rozmiar maksymalnie 2 GB, więc jeśli odzyskiwane dane przekraczają 2 GB, zostaną podzielone na kilka plików PST. Archiwum ZIP będzie chronione ustawionym przez Ciebie hasłem.
8. Otrzymasz wiadomość e-mail z łączem do archiwum ZIP zawierającego utworzone pliki PST.
9. Administrator otrzyma wiadomość e-mail z powiadomieniem o wykonaniu procedury odzyskiwania.

© Acronis International GmbH, 2003-2024

Uwaga
Odzyskiwanie skrzynki pocztowej do plików PST może długo potrwać, ponieważ wiąże się nie tylko z przesyłaniem danych, ale też z ich przekształcaniem przy użyciu złożonych algorytmów.

Aby pobrać archiwum z plikami PST i ukończyć odzyskiwanie

1. Wykonaj jedną z następujących czynności:
   - Aby pobrać archiwum z poziomu wiadomości e-mail, kliknij łącze **Pobierz pliki**.
     Archiwum będzie dostępne do pobrania przez najbliższe 24 godziny. Jeśli łącze wygaśnie, powtórz procedurę odzyskiwania.
   - Aby pobrać archiwum z poziomu konsoli Cyber Protect:
     a. Przejdź do sekcji **Magazyn kopii zapasowych** > **Pliki PST**.
     b. Wybierz najnowsze wyróżnione archiwum.
     c. Kliknij **Pobierz** w prawym okienku.

   Archiwum zostanie pobrane do domyślnego katalogu pobierania na komputerze.
2. Wyodrębnij pliki PST z archiwum przy użyciu hasła ustawionego w celu zaszyfrowania archiwum.
3. Otwórz pliki PST w programie Microsoft Outlook.
   Wynikowe pliki PST mogą mieć znacznie mniejszy rozmiar niż oryginalna skrzynka pocztowa. To normalne.

   Ważne
   Nie importuj tych plików do programu Microsoft Outlook za pomocą narzędzia **Kreator importu i eksportu**.
   W celu otwarcia plików kliknij je dwukrotnie lub kliknij prawym przyciskiem myszy i w menu kontekstowym wybierz **Otwórz za pomocą** > **Microsoft Outlook**.

Odzyskiwanie elementów skrzynki pocztowej do plików PST

Uwaga
W ramach odzyskiwania do plików PST nie można przywrócić archiwum zbiorczego. Jeśli chcesz przywrócić archiwum zbiorcze wraz ze skrzynką pocztową, zobacz sekcję "Odzyskiwanie skrzynek pocztowych" (s. 658).

Aby odzyskać elementy skrzynki pocztowej

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby odzyskać elementy ze skrzynki pocztowej użytkownika, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż użytkownika, którego skrzynka pocztowa pierwotnie zawierała elementy do odzyskania, po czym kliknij **Odzyskiwanie**.

© Acronis International GmbH, 2003-2024

- Aby odzyskać elementy ze współdzielonej skrzynki pocztowej, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż skrzynkę współdzieloną pierwotnie zawierającą elementy, które chcesz odzyskać, i kliknij **Odzyskiwanie**.
- Aby odzyskać elementy ze skrzynki pocztowej grupy, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie wskaż grupę, której skrzynka pocztowa pierwotnie zawierała elementy do odzyskania, po czym kliknij **Odzyskiwanie**.
- Jeśli skrzynka pocztowa użytkownika, grupy lub współdzielona została usunięta, wybierz element w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.

4. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
5. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów.

   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.
   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata, nazwy załącznika i daty.
   - Zdarzenia: wyszukiwanie według tematu i daty.
   - Zadania: wyszukiwanie według tematu i daty.
   - Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.
6. Wybierz elementy, które chcesz odzyskać. Aby mieć możliwość wybrania folderów, kliknij ikonę „Odzyskaj foldery”:

   Możesz również wykonać dowolną z następujących czynności:
   - Po wybraniu elementu kliknij **Pokaż zawartość**, aby zobaczyć jego zawartość, w tym załączniki. Kliknij nazwę załączonego pliku, aby go pobrać.
   - Po zaznaczeniu wiadomości e-mail lub elementu kalendarza możesz kliknąć **Wyślij jako wiadomość e-mail**, aby wysłać ten element na wskazany adres e-mail. Możesz wybrać nadawcę i napisać tekst, który zostanie dołączony do przekazywanego elementu.
   - Tylko w sytuacji, gdy kopia zapasowa nie jest zaszyfrowana, a w wynikach wyszukiwania wybrano jeden element: kliknij **Pokaż wersje**, aby wybrać wersję elementu do odzyskania. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.
7. Kliknij **Odzyskaj jako pliki PST**.
8. Ustaw hasło w celu zaszyfrowania archiwum z plikami PST.

   Hasło powinno się składać z co najmniej jednego znaku.
9. Potwierdź hasło i kliknij **GOTOWE**.

Wybrane elementy skrzynki pocztowej zostaną odzyskane jako pliki danych PST i zarchiwizowane w formacie ZIP. Plik PST może mieć rozmiar maksymalnie 2 GB, więc jeśli odzyskiwane dane przekraczają 2 GB, zostaną podzielone na kilka plików PST. Archiwum ZIP będzie chronione ustawionym przez Ciebie hasłem.

© Acronis International GmbH, 2003-2024

Otrzymasz wiadomość e-mail z łączem do archiwum ZIP zawierającego utworzone pliki PST.

Administrator otrzyma wiadomość e-mail z powiadomieniem o wykonaniu procedury odzyskiwania.

Aby pobrać archiwum z plikami PST i ukończyć odzyskiwanie

1. Wykonaj jedną z następujących czynności:
   - Aby pobrać archiwum z poziomu wiadomości e-mail, kliknij łącze **Pobierz pliki**.
     Archiwum będzie dostępne do pobrania przez najbliższe 24 godziny. Jeśli łącze wygaśnie, powtórz procedurę odzyskiwania.
   - Aby pobrać archiwum z poziomu konsoli Cyber Protect:
     a. Przejdź do sekcji **Magazyn kopii zapasowych** > **Pliki PST**.
     b. Wybierz najnowsze wyróżnione archiwum.
     c. Kliknij **Pobierz** w prawym okienku.

   Archiwum zostanie pobrane do domyślnego katalogu pobierania na komputerze.
2. Wyodrębnij pliki PST z archiwum przy użyciu hasła ustawionego w celu zaszyfrowania archiwum.
3. Otwórz pliki PST w programie Microsoft Outlook.
   Wynikowe pliki PST mogą mieć znacznie mniejszy rozmiar niż oryginalna skrzynka pocztowa. To normalne.

Ważne
Nie importuj tych plików do programu Microsoft Outlook za pomocą narzędzia **Kreator importu i eksportu**.
W celu otwarcia plików kliknij je dwukrotnie lub kliknij prawym przyciskiem myszy i w menu kontekstowym wybierz **Otwórz za pomocą** > **Microsoft Outlook**.

Odzyskiwanie folderów publicznych i elementów folderów

Aby można było odzyskać folder publiczny lub elementy folderu publicznego, co najmniej jeden administrator docelowej organizacji Microsoft 365 musi mieć prawa roli **Właściciel** w odniesieniu do docelowego folderu publicznego. Jeśli odzyskiwanie się nie powiedzie i pojawi się komunikat o błędzie dotyczącym odmowy dostępu, przyznaj te prawa we właściwościach folderu docelowego, wybierz organizację docelową w konsoli Cyber Protect, kliknij **Odśwież**, a następnie ponów operację odzyskiwania.

Aby odzyskać folder publiczny lub elementy folderu

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, rozwiń tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Rozwiń węzeł **Foldery publiczne**, wybierz **Wszystkie foldery publiczne**, wybierz folder publiczny, który chcesz odzyskać lub który pierwotnie zawierał elementy, które chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

© Acronis International GmbH, 2003-2024

- Jeśli folder publiczny został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

  Foldery publiczne można wyszukiwać na podstawie nazwy. Symbole wieloznaczne nie są obsługiwane.

4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj dane**.
6. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów.

   Wiadomości e-mail i posty można wyszukiwać na podstawie tematu, nadawcy, adresata i daty. Symbole wieloznaczne nie są obsługiwane.
7. Wybierz elementy, które chcesz odzyskać. Aby mieć możliwość wybrania folderów, kliknij ikonę „Odzyskaj foldery”:

   Możesz również wykonać dowolną z następujących czynności:
   - Po zaznaczeniu wiadomości e-mail lub posta kliknij **Pokaż zawartość**, aby zobaczyć zawartość wiadomości lub posta, w tym załączniki. Kliknij nazwę załączonego pliku, aby go pobrać.
   - Po zaznaczeniu wiadomości e-mail lub posta kliknij **Wyślij jako wiadomość e-mail**, aby wysłać element na wskazany adres e-mail. Możesz wybrać nadawcę i napisać tekst, który zostanie dołączony do przekazywanego elementu.
   - Tylko w sytuacji, gdy kopia zapasowa nie jest zaszyfrowana, a w wynikach wyszukiwania wybrano jeden element: kliknij **Pokaż wersje**, aby wybrać wersję elementu do odzyskania. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.
8. Kliknij **Odzyskaj**.
9. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.

   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
10. W polu **Odzyskaj do folderu publicznego** wyświetl, zmień lub określ docelowy folder publiczny.

    Domyślnie wybrany jest pierwotny folder. Jeśli folder nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić folder docelowy.

    Podczas odzyskiwania nie można utworzyć nowego folderu publicznego. Aby odzyskać folder publiczny do nowego folderu publicznego, trzeba najpierw utworzyć docelowy folder publiczny w wybranej organizacji Microsoft 365, a następnie pozwolić agentowi w chmurze zsynchronizować zmianę. Agent w chmurze automatycznie synchronizuje się z usługą Microsoft 365 co 24 godziny. Aby niezwłocznie zsynchronizować zmianę, w konsoli Cyber Protect wybierz organizację na stronie **Microsoft 365**, a następnie kliknij **Odśwież**.
11. W polu **Ścieżka** wyświetl lub zmień docelowy podfolder w docelowym folderze publicznym. Domyślnie zostanie odtworzona oryginalna ścieżka.
12. Kliknij **Rozpocznij odzyskiwanie**.

© Acronis International GmbH, 2003-2024

13. Wybierz jedną z następujących opcji zastępowania:

Opcja	Opis
Zastąp istniejące elementy	Wszystkie pliki w lokalizacji docelowej zostaną zastąpione.
Nie zastępuj istniejących elementów	Jeśli lokalizacja docelowa zawiera plik o takiej samej nazwie, nie zostanie on zastąpiony i plik źródłowy nie zostanie zapisany w lokalizacji docelowej.

14. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Ochrona plików z magazynu OneDrive

Jakie elementy można uwzględnić w kopii zapasowej?

Można utworzyć kopię zapasową całego magazynu OneDrive lub znajdujących się w nim poszczególnych plików i folderów.

W planie tworzenia kopii zapasowych jest dostępna osobna opcja, która umożliwia tworzenie kopii zapasowych notesów aplikacji OneNote.

Pliki są zapisywane razem z ich uprawnieniami udostępnienia. Zaawansowane poziomy uprawnień (**Projekt**, **Pełne**, **Wkład**) nie są uwzględniane w kopii zapasowej.

Niektóre pliki mogą zawierać informacje wrażliwe, a dostęp do nich może być blokowany za pomocą reguły zapobiegania utracie danych (DLP) aktywnej w usłudze Microsoft 365. Pliki te nie są uwzględniane w kopii zapasowej, a po zakończeniu operacji tworzenia kopii zapasowej nie są wyświetlane żadne ostrzeżenia.

Ograniczenia

Tworzenie kopii zapasowych zawartości magazynu usługi OneDrive nie jest obsługiwane w przypadku udostępnionych skrzynek pocztowych. Aby utworzyć kopię zapasową tej zawartości, przekonwertuj udostępnioną skrzynkę pocztową na zwykłe konto użytkownika i upewnij się, że usługa OneDrive jest włączona dla tego konta.

Jakie elementy można odzyskać?

Można odzyskać cały magazyn OneDrive lub dowolny plik czy folder, który został uwzględniony w kopii zapasowej.

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

Można wybrać opcję odzyskania uprawnień do udostępniania lub dziedziczenia przez pliki uprawnień z folderu, do którego są odzyskiwane.

Nie można odzyskać łączy umożliwiających udostępnianie plików i folderów.

© Acronis International GmbH, 2003-2024

Wybór plików magazynu OneDrive

Wybierz pliki zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać pliki z magazynu OneDrive

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę organizację, w której przypadku chcesz utworzyć kopię zapasową danych użytkowników. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby tworzyć kopie zapasowe plików wszystkich użytkowników (w tym użytkowników, którzy zostaną utworzeni w przyszłości), rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby tworzyć kopie zapasowe plików wybranych użytkowników, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, następnie wybierz użytkowników, dla których chcesz wykonać kopię zapasową skrzynek pocztowych, po czym kliknij **Kopia zapasowa**.
4. W panelu planu ochrony:
   - Upewnij się, że pozycja **OneDrive** jest zaznaczona w sekcji **Elementy uwzględniane w kopii zapasowej**.

     Jeśli niektórzy z indywidualnie wybranych użytkowników nie mają rozwiązania OneDrive w swoim planie usługi Microsoft 365, nie będzie można wybrać tej opcji.

     Jeśli niektórzy z użytkowników wybranych do kopii zapasowej grupy nie mają usługi OneDrive w swoim planie usługi Microsoft 365, będzie można wybrać tę opcję, ale plan ochrony nie będzie do nich stosowany.
   - W obszarze **Elementy uwzględniane w kopii zapasowej** wykonaj jedną z następujących czynności:
     - Zachowaj ustawienie domyślne **[Wszystkie]** (wszystkie pliki).
     - Określ pliki i foldery do uwzględnienia w kopii zapasowej, dodając ich nazwy lub ścieżki.

       Można używać symboli wieloznacznych (*, ** i ?). Aby uzyskać więcej informacji na temat określania ścieżek i stosowania symboli wieloznacznych, zobacz „Filtry plików”.
     - Określ pliki i foldery do uwzględnienia w kopii zapasowej, przeglądając je.

       Łącze **Przeglądaj** jest dostępne tylko w przypadku tworzenia planu ochrony dla jednego użytkownika.
   - [Opcjonalnie] W obszarze **Elementy uwzględniane w kopii zapasowej** kliknij **Pokaż wykluczenia**, aby określić pliki i foldery, które mają zostać pominięte w procesie tworzenia kopii zapasowej.

     Wykluczenia plików mają wyższy priorytet niż wybór plików, tj. w przypadku wskazania tego samego pliku w obu polach zostanie on pominięty podczas tworzenia kopii zapasowej.
   - [Opcjonalnie] Aby utworzyć kopię zapasową notesów aplikacji OneNote, włącz przełącznik **Uwzględnij aplikację OneNote**.

© Acronis International GmbH, 2003-2024

Odzyskiwanie magazynu OneDrive i plików z magazynu OneDrive

Odzyskiwanie całego dysku OneDrive

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż użytkownika, którego magazyn OneDrive chcesz odzyskać, po czym kliknij **Odzyskiwanie**.
   Jeśli użytkownik został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
   Użytkowników można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

   Uwaga
   Aby wyświetlić wyłącznie punkty odzyskiwania zawierające pliki z magazynu OneDrive, wybierz **OneDrive** w polu **Filtruj według zawartości**.

5. Kliknij **Odzyskaj** > **Cały dysk OneDrive**.
6. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.
   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
   Podczas odzyskiwania nie można utworzyć nowego obiektu docelowego danych usługi OneDrive. Aby odzyskać dane usługi OneDrive do nowego obiektu docelowego, trzeba najpierw utworzyć docelowy obiekt OneDrive w organizacji Microsoft 365, a następnie pozwolić agentowi w chmurze zsynchronizować zmianę. Agent w chmurze automatycznie synchronizuje się z usługą Microsoft 365 co 24 godziny. Aby niezwłocznie zsynchronizować zmianę, w konsoli Cyber Protect wybierz organizację na stronie **Microsoft 365**, a następnie kliknij **Odśwież**.
7. W polu **Odzyskaj na dysk** wyświetl, zmień lub określ użytkownika docelowego.
   Domyślnie jest wybrany pierwotny użytkownik. Jeśli użytkownik nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelowego użytkownika.
8. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania plików.
9. Kliknij **Rozpocznij odzyskiwanie**.
10. Wybierz jedną z następujących opcji zastępowania:

Opcja	Opis
Zastąp istniejący plik, jeśli jest starszy	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie jak plik źródłowy, ale starszy od niego, plik źródłowy zostanie zapisany w lokalizacji docelowej, zastępując starszą wersję.

© Acronis International GmbH, 2003-2024

Opcja	Opis
Zastąp istniejące pliki	Wszystkie pliki w lokalizacji docelowej zostaną zastąpione, niezależnie od daty ich ostatniej modyfikacji.
Nie zastępuj istniejących plików	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie, nie zostaną do niego zastosowane żadne zmiany, a plik źródłowy nie zostanie zapisany w lokalizacji docelowej.

Uwaga
W przypadku odzyskiwania notesów aplikacji OneNote użycie zarówno opcji **Zastąp istniejący plik, jeśli jest starszy**, jak i opcji **Zastąp istniejące pliki** będzie powodować zastępowanie istniejących już notesów aplikacji OneNote.

11. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Odzyskiwanie plików z magazynu OneDrive

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie wskaż użytkownika, którego pliki z magazynu OneDrive chcesz odzyskać, po czym kliknij **Odzyskiwanie**.
   Jeśli użytkownik został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
   Użytkowników można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

Uwaga
Aby wyświetlić wyłącznie punkty odzyskiwania zawierające pliki z magazynu OneDrive, wybierz **OneDrive** w polu **Filtruj według zawartości**.

5. Kliknij **Odzyskaj** > **Pliki/foldery**.
6. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych plików i folderów.
7. Wybierz pliki, które chcesz odzyskać.
   Jeśli kopia zapasowa nie jest zaszyfrowana i wybrano jeden plik, możesz kliknąć **Pokaż wersje**, aby wybrać wersję pliku do odzyskania. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.
8. Jeśli chcesz pobrać plik, zaznacz go, kliknij **Pobierz**, wybierz lokalizację, w której ma zostać zapisany plik, i kliknij **Zapisz**. W przeciwnym razie pomiń ten krok.
9. Kliknij **Odzyskaj**.

© Acronis International GmbH, 2003-2024

10. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.

    Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.

    Podczas odzyskiwania nie można utworzyć nowego obiektu OneDrive. Aby odzyskać plik do nowego obiektu OneDrive, trzeba najpierw utworzyć docelowy obiekt OneDrive w wybranej organizacji Microsoft 365, a następnie pozwolić agentowi w chmurze zsynchronizować zmianę. Agent w chmurze automatycznie synchronizuje się z usługą Microsoft 365 co 24 godziny. Aby niezwłocznie zsynchronizować zmianę, w konsoli Cyber Protect wybierz organizację na stronie **Microsoft 365**, a następnie kliknij **Odśwież**.
11. W polu **Odzyskaj na dysk** wyświetl, zmień lub określ użytkownika docelowego.

    Domyślnie jest wybrany pierwotny użytkownik. Jeśli użytkownik nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić użytkownika docelowego.
12. W sekcji **Ścieżka** wyświetl lub zmień folder docelowy w magazynie OneDrive docelowego użytkownika. Domyślnie jest wybrana pierwotna lokalizacja.
13. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania plików.
14. Kliknij **Rozpocznij odzyskiwanie**.
15. Wybierz jedną z następujących opcji zastępowania plików:

Opcja	Opis
Zastąp istniejący plik, jeśli jest starszy	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie jak plik źródłowy, ale starszy od niego, plik źródłowy zostanie zapisany w lokalizacji docelowej, zastępując starszą wersję.
Zastąp istniejące pliki	Wszystkie pliki w lokalizacji docelowej zostaną zastąpione, niezależnie od daty ich ostatniej modyfikacji.
Nie zastępuj istniejących plików	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie, nie zostaną do niego zastosowane żadne zmiany, a plik źródłowy nie zostanie zapisany w lokalizacji docelowej.

    Uwaga
    W przypadku odzyskiwania notesów aplikacji OneNote użycie zarówno opcji **Zastąp istniejący plik, jeśli jest starszy**, jak i opcji **Zastąp istniejące pliki** będzie powodować zastępowanie istniejących już notesów aplikacji OneNote.
16. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Ochrona witryn programu SharePoint Online

Jakie elementy można uwzględnić w kopii zapasowej?

W kopii zapasowej można uwzględnić zbiory klasycznych witryn SharePoint, witryny grup (nowoczesne witryny zespołów) i witryny służące do komunikacji. Można też uwzględniać

© Acronis International GmbH, 2003-2024

poszczególne podwitryny, listy i biblioteki.

W planie tworzenia kopii zapasowych jest dostępna osobna opcja, która umożliwia tworzenie kopii zapasowych notesów aplikacji OneNote.

Podczas tworzenia kopii zapasowej są *pomijane* następujące elementy:

- Ustawienia witryny z kategorii **Wygląd i działanie** (oprócz **tytułu, opisu i logo**).
- Komentarze na stronach witryny oraz ustawienia tych komentarzy (**włączanie**/**wyłączanie** komentarzy).
- Ustawienia witryny **Funkcje witryny**.
- Strony składników Web Part oraz składniki Web Part wbudowane w strony wiki (z uwagi na ograniczenia API SharePoint Online).
- Wyewidencjonowane pliki — pliki ręcznie wyewidencjonowane do edycji oraz wszystkie pliki utworzone lub przesłane w bibliotekach, w których przypadku jest włączona opcja **Wymagaj wyewidencjonowania**. Aby utworzyć kopię zapasową tych plików, należy je najpierw zaewidencjonować.
- Kolumny typu „Dane zewnętrzne" i „Zarządzane metadane".
- Domyślny zbiór witryn „domain-my.sharepoint.com". Jest to zbiór plików z dysków OneDrive wszystkich użytkowników należących do organizacji.
- Zawartość kosza.

Ograniczenia

- Jeśli rozmiar tytułów i opisów witryn, podwitryn, list oraz kolumn przekracza 10 000 bajtów, są one obcinane w trakcie tworzenia kopii zapasowych.
- Nie można tworzyć kopii zapasowych poprzednich wersji plików utworzonych w programie SharePoint Online. Są chronione tylko ich najnowsze wersje.
- Nie można utworzyć kopii zapasowej biblioteki archiwum.
- Nie można tworzyć kopii zapasowych witryn utworzonych w pakiecie Business Productivity Online Suite (BPOS), poprzedniku usługi Microsoft 365.
- Nie można tworzyć kopii zapasowych ustawień witryn, które korzystają ze ścieżki zarządzanej `/portals` (na przykład `https://<dzierżawca>.sharepoint.com/portals/...`).
- Ustawienia usługi Zarządzanie prawami do informacji dotyczące listy lub biblioteki można odzyskać tylko wtedy, gdy usługa ta jest włączona w docelowej organizacji Microsoft 365.

Jakie elementy można odzyskać?

Z kopii zapasowej witryny można odzyskać następujące elementy:

- Cała witryna
- Podwitryny
- Listy
- Elementy z list

© Acronis International GmbH, 2003-2024

- Biblioteki dokumentów
- Dokumenty
- Załączniki do elementów list
- Strony zwykłe i wiki

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

Elementy mogą zostać odzyskane na pierwotną lub nową witrynę. Ścieżka odzyskanego elementu jest taka sama jak pierwotnego. Jeśli ścieżka nie istnieje, zostanie utworzona.

Można wybrać opcję odzyskania uprawnień do udostępniania lub dziedziczenia przez elementy uprawnień z obiektu nadrzędnego po odzyskaniu.

Które elementy są nieodzyskiwalne?

- Podwitryny oparte na szablonie **Repozytorium procesów Visio**.
- Listy następujących typów: **lista ankiet**, **lista zadań**, **biblioteka obrazów**, **łącza**, **kalendarz**, **tablica dyskusyjna**, **elementy zewnętrzne** i **import arkusza kalkulacyjnego**.
- Listy, dla których włączone jest wiele rodzajów zawartości.

Wybór danych programu SharePoint Online

Wybierz dane zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać dane programu SharePoint Online

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę organizację, w której przypadku chcesz utworzyć kopię zapasową danych użytkowników. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby tworzyć kopie zapasowe wszystkich klasycznych witryn SharePoint w organizacji (w tym witryn, które zostaną utworzone w przyszłości), rozwiń węzeł **Zbiory witryn**, wybierz opcję **Wszystkie zbiory witryn**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby odzyskać wybrane witryny klasyczne, rozwiń węzeł **Zbiory witryn**, wybierz opcję **Wszystkie zbiory witryn**, następnie wskaż witrynę, którą chcesz zapisać, po czym kliknij **Kopia zapasowa**.
   - Aby tworzyć kopie zapasowe wszystkich witryn grup (nowoczesnych witryn zespołów), w tym witryn, które zostaną utworzone w przyszłości, rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby tworzyć kopie zapasowe wybranych witryn grup (nowoczesnych witryn zespołów), rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, następnie wskaż grupy, w których przypadku chcesz wykonać kopię zapasową witryn, po czym kliknij **Kopia zapasowa**.
4. W panelu planu ochrony:

© Acronis International GmbH, 2003-2024

- Upewnij się, że pozycja **Witryny SharePoint** jest zaznaczona w sekcji **Elementy uwzględniane w kopii zapasowej**.
- W obszarze **Elementy uwzględniane w kopii zapasowej** wykonaj jedną z następujących czynności:
  - Zachowaj ustawienie domyślne **[Wszystkie]** (wszystkie pliki z wybranych witryn).
  - Określ podwitryny, listy i biblioteki do uwzględnienia w kopii zapasowej, dodając ich nazwy lub ścieżki.

    Aby utworzyć kopię zapasową podwitryny lub listy/biblioteki witryny najwyższego poziomu, określ nazwę wyświetlaną tego elementu w następującym formacie: `/nazwa wyświetlana/**`

    Aby utworzyć kopię zapasową listy/biblioteki podwitryny, określ nazwę wyświetlaną tego elementu w następującym formacie: `/nazwa wyświetlana podwitryny/nazwa wyświetlana listy/**`

    Nazwy wyświetlane podwitryn, list i bibliotek znajdują się na stronie **Zawartość witryny** każdej witryny lub podwitryny SharePoint.
  - Określ podwitryny do uwzględnienia w kopii zapasowej, przeglądając je.

    Łącze **Przeglądaj** jest dostępne tylko w przypadku tworzenia planu ochrony dla jednej witryny.
- [Opcjonalnie] W sekcji **Elementy uwzględniane w kopii zapasowej** kliknij **Pokaż wykluczenia**, aby określić podwitryny, listy i biblioteki, które mają zostać pominięte w procesie tworzenia kopii zapasowej.

  Wykluczenia elementów mają wyższy priorytet niż wybór elementów, tj. w przypadku wskazania tej samej podwitryny w obu polach zostanie ona pominięta podczas tworzenia kopii zapasowej.
- [Opcjonalnie] Aby utworzyć kopię zapasową notesów aplikacji OneNote, włącz przełącznik **Uwzględnij aplikację OneNote**.

Odzyskiwanie danych z programu SharePoint Online

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby odzyskać dane z witryny grupy (nowoczesnej witryny zespołu), rozwiń węzeł **Grupy**, wybierz opcję **Wszystkie grupy**, a następnie wskaż grupę, której witryna pierwotnie zawierała elementy do odzyskania, po czym kliknij **Odzyskiwanie**.
   - Aby odzyskać elementy z witryny klasycznej, rozwiń węzeł **Zbiory witryn**, wybierz opcję **Wszystkie zbiory witryn**, a następnie wskaż witrynę, która pierwotnie zawierała elementy do odzyskania, po czym kliknij **Odzyskiwanie**.
   - Jeśli witryna została usunięta, wybierz ją w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

   Grupy i witryny można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

© Acronis International GmbH, 2003-2024

Uwaga
Aby wyświetlić wyłącznie punkty odzyskiwania zawierające witryny SharePoint, wybierz opcję **Witryny SharePoint** w sekcji **Filtruj według zawartości**.

5. Kliknij **Odzyskaj pliki programu SharePoint**.
6. Przejdź do właściwego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów danych.
7. Wybierz elementy, które chcesz odzyskać.

   Jeśli kopia zapasowa nie jest zaszyfrowana, a w wynikach wyszukiwania wybrano jeden element, możesz kliknąć **Pokaż wersje**, aby wybrać wersję elementu do odzyskania. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.
8. [Opcjonalnie] Aby pobrać element, zaznacz go, kliknij **Pobierz**, wybierz lokalizację, w której ma zostać zapisany ten element, i kliknij **Zapisz**.
9. Kliknij **Odzyskaj**.
10. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.

    Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
11. W polu **Odzyskaj do witryny** wyświetl, zmień lub określ witrynę docelową.

    Podczas odzyskiwania nie można utworzyć nowej witryny programu SharePoint. Aby odzyskać witrynę programu SharePoint do nowej takiej witryny, trzeba najpierw utworzyć witrynę docelową w odpowiedniej organizacji Microsoft 365, a następnie pozwolić agentowi w chmurze zsynchronizować zmianę. Agent w chmurze automatycznie synchronizuje się z usługą Microsoft 365 co 24 godziny. Aby niezwłocznie zsynchronizować zmianę, w konsoli Cyber Protect wybierz organizację na stronie **Microsoft 365**, a następnie kliknij **Odśwież**.
12. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania odzyskiwanych plików.
13. Kliknij **Rozpocznij odzyskiwanie**.
14. Wybierz jedną z następujących opcji zastępowania:

Opcja	Opis
Zastąp istniejący plik, jeśli jest starszy	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie jak plik źródłowy, ale starszy od niego, plik źródłowy zostanie zapisany w lokalizacji docelowej, zastępując starszą wersję.
Zastąp istniejące pliki	Wszystkie pliki w lokalizacji docelowej zostaną zastąpione, niezależnie od daty ich ostatniej modyfikacji.
Nie zastępuj istniejących plików	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie, nie zostaną do niego zastosowane żadne zmiany, a plik źródłowy nie zostanie zapisany w lokalizacji docelowej.

© Acronis International GmbH, 2003-2024

Uwaga
W przypadku odzyskiwania notesów aplikacji OneNote użycie zarówno opcji **Zastąp istniejący plik, jeśli jest starszy**, jak i opcji **Zastąp istniejące pliki** będzie powodować zastępowanie istniejących już notesów aplikacji OneNote.

15. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Ochrona instancji Microsoft 365 Teams

Jakie elementy można uwzględnić w kopii zapasowej?

W kopii zapasowej można uwzględniać całe zespoły. Obejmuje to nazwę zespołu, listę członków zespołu, kanały zespołu wraz z ich zawartością, skrzynkę pocztową i spotkania zespołu oraz witrynę zespołu.

W planie tworzenia kopii zapasowych jest dostępna osobna opcja, która umożliwia tworzenie kopii zapasowych notesów aplikacji OneNote.

Jakie elementy można odzyskać?

- Cały zespół
- Kanały zespołu
- Pliki z kanałów
- Skrzynka pocztowa zespołu
- Foldery poczty e-mail w skrzynce pocztowej zespołu
- Wiadomości e-mail w skrzynce pocztowej zespołu
- Spotkania
- Witryna zespołu

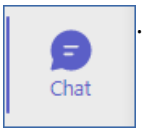
Nie można odzyskać konwersacji z kanałów zespołu, ale można je pobrać jako jeden plik html.

Ograniczenia

W kopii zapasowej nie są uwzględniane następujące elementy:

- Ustawienia kanału ogólnego (preferencje moderacji) — ze względu na ograniczenia interfejsu API Microsoft Teams w wersji beta.
- Ustawienia kanałów niestandardowych (preferencje moderacji) — ze względu na ograniczenia interfejsu API Microsoft Teams w wersji beta.
- Notatki ze spotkań.

© Acronis International GmbH, 2003-2024

- Wiadomości w sekcji czatu 

. Ta sekcja zawiera prywatne czaty z indywidualnymi osobami i czaty grupowe.
- Naklejki i pochwały.

Tworzenie kopii zapasowych i odzyskiwanie są obsługiwane w przypadku następujących kart kanałów:

- Word
- Excel
- PowerPoint
- PDF
- Biblioteka dokumentów

Wybieranie zespołów

Wybierz zespoły zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać zespoły

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której zespoły chcesz uwzględnić w kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby tworzyć kopie zapasowe wszystkich zespołów organizacji (w tym zespołów, które zostaną utworzone w przyszłości), rozwiń węzeł **Zespoły**, zaznacz opcję **Wszystkie zespoły**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby tworzyć kopie zapasowe pojedynczych zespołów, rozwiń węzeł **Zespoły**, zaznacz opcję **Wszystkie zespoły**, następnie wskaż zespoły, które chcesz uwzględnić w kopii zapasowej, i kliknij **Kopia zapasowa**.

   Zespoły można wyszukiwać po nazwach. Symbole wieloznaczne nie są obsługiwane.
4. W panelu planu ochrony:
   - Upewnij się, że w obszarze **Elementy uwzględniane w kopii zapasowej** jest zaznaczona pozycja **Microsoft Teams**.
   - [Opcjonalnie] W polu **Okres przechowywania** ustaw opcje czyszczenia.
   - [Opcjonalnie] Jeśli chcesz zaszyfrować kopię zapasową, włącz przełącznik **Szyfrowanie**, a następnie ustaw hasło i wybierz algorytm szyfrowania.
   - [Opcjonalnie] Aby utworzyć kopię zapasową notesów aplikacji OneNote, włącz przełącznik **Uwzględnij aplikację OneNote**.

© Acronis International GmbH, 2003-2024

Odzyskiwanie całego zespołu

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której zespoły chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Zespoły**, wybierz **Wszystkie zespoły**, wskaż zespół, który chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

   Zespoły można wyszukiwać po nazwach. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Cały zespół**.

   Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.

   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
6. W polu **Odzyskaj do zespołu** wyświetl zespół docelowy lub wybierz inny.

   Domyślnie jest wybrany pierwotny zespół. Jeśli ten zespół nie istnieje (na przykład został usunięty) lub wybrano organizację, która nie zawiera pierwotnego zespołu, trzeba wybrać zespół docelowy z listy rozwijanej.

   Zespół można odzyskać tylko do już istniejącego zespołu. Nie można tworzyć zespołów podczas operacji odzyskiwania.
7. Kliknij **Rozpocznij odzyskiwanie**.
8. Wybierz jedną z następujących opcji zastępowania:
   - **Zastąp istniejącą zawartość, jeśli jest starsza**
   - **Zastąp istniejącą zawartość**
   - **Nie zastępuj istniejącej zawartości**

   Uwaga
   W przypadku odzyskiwania notesów aplikacji OneNote użycie zarówno opcji **Zastąp istniejącą zawartość, jeśli jest starsza**, jak i opcji **Zastąp istniejącą zawartość** będzie powodować zastępowanie istniejących już notesów aplikacji OneNote.
9. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Gdy usuniesz kanał w interfejsie graficznym Microsoft Teams, nie jest on natychmiast usuwany z systemu. Gdy więc odzyskujesz cały zespół, nie można użyć nazwy tego kanału, w związku z czym zostanie do niej dodany postfiks.

Konwersacje są odzyskiwane jako jeden plik html na karcie **Pliki** kanału. Plik ten można znaleźć w folderze o nazwie zgodnej z poniższym wzorcem: `<Nazwa zespołu>_<Nazwa kanału>_conversations_backup_<data odzyskania>T<godzina odzyskania>Z`.

© Acronis International GmbH, 2003-2024

Uwaga
Po odzyskaniu zespołu lub kanałów zespołu przejdź do Microsoft Teams, zaznacz odzyskane kanały, a następnie kliknij ich kartę **Pliki**. W przeciwnym razie w kolejnych kopiach zapasowych tych kanałów nie będzie uwzględniana zawartość tej karty — ze względu na ograniczenia interfejsu API Microsoft Teams w wersji beta.

Odzyskiwanie kanałów zespołu lub dostępnych w nich plików

Aby odzyskać kanały zespołu

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której zespoły chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Zespoły**, wybierz **Wszystkie zespoły**, wskaż zespół, którego kanały chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Kanały**.
6. Wybierz kanały, które chcesz odzyskać, a następnie kliknij **Odzyskaj**. Aby wybrać kanał w głównym okienku, zaznacz pole wyboru przed jego nazwą.
   Dostępne są następujące opcje wyszukiwania:
   - **Konwersacje**: nadawca, temat, zawartość, język, nazwa załącznika, data lub zakres dat.
   - **Pliki**: nazwa pliku lub folderu, typ pliku, rozmiar, data lub zakres dat ostatniej zmiany.

   Uwaga
   Zamiast odzyskać pliki, można je też pobrać lokalnie.
7. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.
   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
8. W polu **Odzyskaj do zespołu** wyświetl, zmień lub określ zespół docelowy.
   Domyślnie jest wybrany pierwotny zespół. Jeśli zespół nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić zespół docelowy.
9. W polu **Odzyskaj do kanału** wyświetl, zmień lub określ kanał docelowy.
10. Kliknij **Rozpocznij odzyskiwanie**.
11. Wybierz jedną z następujących opcji zastępowania:
    - **Zastąp istniejącą zawartość, jeśli jest starsza**
    - **Zastąp istniejącą zawartość**
    - **Nie zastępuj istniejącej zawartości**

© Acronis International GmbH, 2003-2024

Uwaga
W przypadku odzyskiwania notesów aplikacji OneNote użycie zarówno opcji **Zastąp istniejącą zawartość, jeśli jest starsza**, jak i opcji **Zastąp istniejącą zawartość** będzie powodować zastępowanie istniejących już notesów aplikacji OneNote.

12. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Konwersacje są odzyskiwane jako jeden plik html na karcie **Pliki** kanału. Plik ten można znaleźć w folderze o nazwie zgodnej z poniższym wzorcem: `<Nazwa zespołu>_<Nazwa kanału>_conversations_backup_<data odzyskania>T<godzina odzyskania>Z`.

Uwaga
Po odzyskaniu zespołu lub kanałów zespołu przejdź do Microsoft Teams, zaznacz odzyskane kanały, a następnie kliknij ich kartę **Pliki**. W przeciwnym razie w kolejnych kopiach zapasowych tych kanałów nie będzie uwzględniana zawartość tej karty — ze względu na ograniczenia interfejsu API Microsoft Teams w wersji beta.

Aby odzyskać pliki z kanału zespołu

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której zespoły chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Zespoły**, wybierz **Wszystkie zespoły**, wskaż zespół, którego kanały chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Kanały**.
6. Zaznacz odpowiedni kanał, a następnie otwórz folder **Pliki**.
   Przejdź do potrzebnych elementów lub skorzystaj z funkcji wyszukiwania, aby uzyskać ich listę. Dostępne są następujące opcje wyszukiwania: nazwa pliku lub folderu, typ pliku, jego rozmiar, data lub zakres dat ostatniej zmiany.
7. [Opcjonalnie] Aby pobrać element, zaznacz go, kliknij **Pobierz**, wybierz lokalizację, w której ma zostać zapisany ten element, i kliknij **Zapisz**.
8. Wybierz elementy, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
9. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij Organizacja Microsoft 365, aby wyświetlić, zmienić lub określić organizację docelową.
   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
10. W polu **Odzyskaj do zespołu** wyświetl, zmień lub określ zespół docelowy.
    Domyślnie jest wybrany pierwotny zespół. Jeśli zespół nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić zespół docelowy.
11. W polu **Odzyskaj do kanału** wyświetl, zmień lub określ kanał docelowy.

© Acronis International GmbH, 2003-2024

12. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania odzyskiwanych plików.
13. Kliknij **Rozpocznij odzyskiwanie**.
14. Wybierz jedną z następujących opcji zastępowania:
    - **Zastąp istniejącą zawartość, jeśli jest starsza**
    - **Zastąp istniejącą zawartość**
    - **Nie zastępuj istniejącej zawartości**

    Uwaga
    W przypadku odzyskiwania notesów aplikacji OneNote użycie zarówno opcji **Zastąp istniejącą zawartość, jeśli jest starsza**, jak i opcji **Zastąp istniejącą zawartość** będzie powodować zastępowanie istniejących już notesów aplikacji OneNote.
15. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Nie można odzyskiwać pojedynczych konwersacji. W głównym okienku możesz tylko przeglądać folder **Konwersacje** lub pobrać jego zawartość jako jeden plik html. W tym celu kliknij ikonę „odzyskaj foldery” , zaznacz odpowiedni folder **Konwersacje** i kliknij **Pobierz**.

Możesz też wyszukiwać wiadomości w folderze **Konwersacji** według następujących kryteriów:

- Nadawca
- Zawartość
- Nazwa załącznika
- Data

Odzyskiwanie skrzynki pocztowej zespołu

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której zespoły chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Zespoły**, wybierz **Wszystkie zespoły**, wskaż zespół, którego skrzynkę pocztową chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
   Zespoły można wyszukiwać po nazwach. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
6. Kliknij ikonę „odzyskaj foldery” , zaznacz odpowiedni folder skrzynki pocztowej i kliknij **Odzyskaj**.

   Uwaga
   Możesz też odzyskać wybrany folder z wybranej skrzynki pocztowej.

© Acronis International GmbH, 2003-2024

7. Kliknij **Odzyskaj**.
8. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.

   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
9. W polu **Odzyskaj do skrzynki pocztowej** wyświetl, zmień lub określ docelową skrzynkę pocztową.

   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelową skrzynkę pocztową.
10. Kliknij **Rozpocznij odzyskiwanie**.
11. Wybierz jedną z następujących opcji zastępowania:
    - **Zastąp istniejące elementy**
    - **Nie zastępuj istniejących elementów**
12. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Odzyskiwanie elementów skrzynki pocztowej zespołu do plików PST

Aby odzyskać elementy skrzynki pocztowej zespołu

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Rozwiń węzeł **Teams**, wybierz **Wszystkie zespoły**, wskaż zespół, którego skrzynka pocztowa pierwotnie zawierała elementy do odzyskania, a następnie kliknij **Odzyskiwanie**.
5. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
6. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów.

   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.
   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata, nazwy załącznika i daty.
   - Zdarzenia: wyszukiwanie według tematu i daty.
   - Zadania: wyszukiwanie według tematu i daty.
   - Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.
7. Wybierz elementy, które chcesz odzyskać. Aby mieć możliwość wybrania folderów, kliknij ikonę „Odzyskaj foldery”:

   Możesz również wykonać dowolną z następujących czynności:
   - Po wybraniu elementu kliknij **Pokaż zawartość**, aby zobaczyć jego zawartość, w tym załączniki. Kliknij nazwę załączonego pliku, aby go pobrać.

© Acronis International GmbH, 2003-2024

- Po zaznaczeniu wiadomości e-mail lub elementu kalendarza możesz kliknąć **Wyślij jako wiadomość e-mail**, aby wysłać ten element na wskazany adres e-mail. Możesz wybrać nadawcę i napisać tekst, który zostanie dołączony do przekazywanego elementu.
- Jeśli kopia zapasowa nie jest zaszyfrowana, a w wynikach wyszukiwania wybrano jeden element: kliknij **Pokaż wersje**, aby wyświetlić wersję elementu. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej, bez względu na to, czy została ona utworzona przed wybranym punktem odzyskiwania, czy później.

8. Kliknij **Odzyskaj jako pliki PST**.
9. Ustaw hasło w celu zaszyfrowania archiwum z plikami PST.
   Hasło powinno się składać z co najmniej jednego znaku.
10. Potwierdź hasło i kliknij **GOTOWE**.

Wybrane elementy skrzynki pocztowej zostaną odzyskane jako pliki danych PST i zarchiwizowane w formacie ZIP. Plik PST może mieć rozmiar maksymalnie 2 GB, więc jeśli odzyskiwane dane przekraczają 2 GB, zostaną podzielone na kilka plików PST. Archiwum ZIP będzie chronione ustawionym przez Ciebie hasłem.

Otrzymasz wiadomość e-mail z łączem do archiwum ZIP zawierającego utworzone pliki PST.

Administrator otrzyma wiadomość e-mail z powiadomieniem o wykonaniu procedury odzyskiwania.

Aby pobrać archiwum z plikami PST i ukończyć odzyskiwanie

1. Wykonaj jedną z następujących czynności:
   - Aby pobrać archiwum z poziomu wiadomości e-mail, kliknij łącze **Pobierz pliki**.
     Archiwum będzie dostępne do pobrania przez najbliższe 24 godziny. Jeśli łącze wygaśnie, powtórz procedurę odzyskiwania.
   - Aby pobrać archiwum z poziomu konsoli Cyber Protect:
     a. Przejdź do sekcji **Magazyn kopii zapasowych** > **Pliki PST**.
     b. Wybierz najnowsze wyróżnione archiwum.
     c. Kliknij **Pobierz** w prawym okienku.

   Archiwum zostanie pobrane do domyślnego katalogu pobierania na komputerze.
2. Wyodrębnij pliki PST z archiwum przy użyciu hasła ustawionego w celu zaszyfrowania archiwum.
3. W programie Microsoft Outlook otwórz lub zaimportuj pliki PST. Aby się dowiedzieć, jak to zrobić, zapoznaj się z dokumentacją firmy Microsoft.

Odzyskiwanie wiadomości e-mail i spotkań

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której zespoły chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Zespoły**, wybierz **Wszystkie zespoły**, wskaż zespół, którego wiadomości e-mail lub spotkania chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

© Acronis International GmbH, 2003-2024

Zespoły można wyszukiwać po nazwach. Symbole wieloznaczne nie są obsługiwane.

4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
6. Przejdź do potrzebnego elementu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów.

   Dostępne są następujące opcje wyszukiwania:

   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata i daty.
   - Spotkania: wyszukiwanie według nazwy i daty wydarzenia.
7. Wybierz elementy, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.

   Uwaga
   Spotkania można znaleźć w folderze **Kalendarz**.

   Możesz również wykonać dowolną z następujących czynności:

   - Po wybraniu elementu kliknij **Pokaż zawartość**, aby zobaczyć jego zawartość, w tym załączniki. Kliknij nazwę załączonego pliku, aby go pobrać.
   - Po zaznaczeniu wiadomości e-mail lub spotkania możesz kliknąć **Wyślij jako wiadomość e-mail**, aby wysłać dany element na wskazany adres e-mail. Możesz wybrać nadawcę i napisać tekst, który zostanie dołączony do przekazywanego elementu.
8. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.

   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
9. W polu **Odzyskaj do skrzynki pocztowej** wyświetl, zmień lub określ docelową skrzynkę pocztową.

   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelową skrzynkę pocztową.
10. Kliknij **Rozpocznij odzyskiwanie**.
11. Wybierz jedną z następujących opcji zastępowania:
    - **Zastąp istniejące elementy**
    - **Nie zastępuj istniejących elementów**
12. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Odzyskiwanie witryny zespołu lub poszczególnych elementów witryny

1. Kliknij **Microsoft 365**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, wybierz tę, której zespoły chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Zespoły**, wybierz **Wszystkie zespoły**, wskaż zespół, którego witrynę chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

© Acronis International GmbH, 2003-2024

Zespoły można wyszukiwać po nazwach. Symbole wieloznaczne nie są obsługiwane.

4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Witryna zespołu**.
6. Przejdź do potrzebnego elementu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów.
7. [Opcjonalnie] Aby pobrać element, zaznacz go, kliknij **Pobierz**, wybierz lokalizację, w której ma zostać zapisany ten element, i kliknij **Zapisz**.
8. Wybierz elementy, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
9. Jeśli do usługi Cyber Protection dodano wiele organizacji Microsoft 365, kliknij **Organizacja Microsoft 365**, aby wyświetlić, zmienić lub określić organizację docelową.

   Domyślnie wybrane są pierwotna organizacja i pierwotny zespół. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wskazać organizację docelową.
10. W polu **Odzyskaj do zespołu** wyświetl, zmień lub określ zespół docelowy.

    Domyślnie jest wybrany pierwotny zespół. Jeśli zespół nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić witrynę docelową.
11. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania odzyskiwanych plików.
12. Kliknij **Rozpocznij odzyskiwanie**.
13. Wybierz jedną z następujących opcji zastępowania:
    - **Zastąp istniejącą zawartość, jeśli jest starsza**
    - **Zastąp istniejącą zawartość**
    - **Nie zastępuj istniejącej zawartości**

    Uwaga
    W przypadku odzyskiwania notesów aplikacji OneNote użycie zarówno opcji **Zastąp istniejącą zawartość, jeśli jest starsza**, jak i opcji **Zastąp istniejącą zawartość** będzie powodować zastępowanie istniejących już notesów aplikacji OneNote.
14. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Ochrona notesów aplikacji OneNote

Domyślnie notesy programu OneNote są uwzględniane w kopiach zapasowych plików programu OneDrive, programu Microsoft Teams i witryn SharePoint.

Aby wykluczyć notesy programu OneNote z tych kopii zapasowych, wyłącz przełącznik **Uwzględnij aplikację OneNote** w odpowiednim planie tworzenia kopii zapasowych.

Odzyskiwanie notesów aplikacji OneNote uwzględnionych w kopii zapasowej

Aby się dowiedzieć, jak odzyskać notes aplikacji OneNote uwzględniony w kopii zapasowej, zapoznaj się z odpowiednim tematem:

© Acronis International GmbH, 2003-2024

- W przypadku kopii zapasowej dysku OneDrive zobacz "Odzyskiwanie całego dysku OneDrive" (s. 668) lub "Odzyskiwanie plików z magazynu OneDrive" (s. 669).
- W przypadku kopii zapasowej danych programu Teams zobacz "Odzyskiwanie całego zespołu" (s. 677), "Odzyskiwanie kanałów zespołu lub dostępnych w nich plików" (s. 678) lub "Odzyskiwanie witryny zespołu lub poszczególnych elementów witryny" (s. 683).
- W przypadku kopii zapasowej witryny programu SharePoint zobacz "Odzyskiwanie danych z programu SharePoint Online" (s. 673).

Obsługiwane wersje

- OneNote (OneNote 2016 lub nowszy)
- OneNote dla systemu Windows 10

Ograniczenia i znane problemy

- W przypadku notesów programu OneNote zapisywanych w usłudze OneDrive lub programie SharePoint obowiązuje ograniczenie do 2 GB. Większych notesów programu OneNote nie można odzyskać do obiektów docelowych OneDrive lub SharePoint.
- Notesy aplikacji OneNote z grupami sekcji nie są obsługiwane.
- W uwzględnionych w kopii zapasowej notesach aplikacji OneNote, które zawierają sekcje o nazwach innych niż domyślne, pierwsza sekcja jest wyświetlana z nazwą domyślną (np. `Nowa sekcja` lub `Sekcja bez tytułu`). Może to mieć wpływ na kolejność sekcji w notesach z wieloma sekcjami.
- W przypadku odzyskiwania notesów aplikacji OneNote użycie zarówno opcji **Zastąp istniejącą zawartość, jeśli jest starsza**, jak i opcji **Zastąp istniejącą zawartość** będzie powodować zastępowanie istniejących już notesów aplikacji OneNote.
- Jeśli odzyskujesz cały zespół, witrynę zespołu lub folder `Elementy zawartości witryny` z witryny zespołu i wybierzesz opcję **Zastąp istniejącą zawartość, jeśli jest starsza** lub **Zastąp istniejącą zawartość**, domyślny notes aplikacji OneNote tego zespołu nie zostanie zastąpiony. Odzyskiwanie przebiegnie pomyślnie, ale zakończy się ostrzeżeniem: *Nie można zaktualizować właściwości pliku „/sites/<nazwa zespołu>/SiteAssets/<nazwa notesu aplikacji OneNote>”*.

Ochrona stanowisk aplikacji do współpracy Microsoft 365

Możesz skorzystać z pakietu Advanced Email Security, który umożliwia chronienie skrzynek pocztowych Microsoft 365, Google Workspace lub Open-Xchange w czasie rzeczywistym:

- Ochrona przed złośliwym oprogramowaniem i Ochrona przed spamem
- Skanowanie adresów URL w wiadomościach e-mail
- Analiza DMARC
- Ochrona przed phishingiem
- Ochrona przed podszywaniem się
- Skanowanie załączników

© Acronis International GmbH, 2003-2024

- Rozbrajanie i rekonstrukcja zawartości
- Schemat relacji zaufania

Możesz też włączyć stanowiska aplikacji do współpracy Microsoft 365, co umożliwi chronienie chmurowych aplikacji do współpracy Microsoft 365 przed zagrożeniami związanymi z zawartością. Do tych aplikacji należą OneDrive, SharePoint i Teams.

Moduł Advanced Email Security może być udostępniany na obciążenie lub na gigabajt i będzie miała wpływ na model licencjonowania.

Aby przejść do wprowadzenia dla użytkownika pakietu Advanced Email Security z poziomu konsoli Cyber Protect Cloud

1. Kliknij **Urządzenia** > **Microsoft 365**.
2. Kliknij węzeł **Użytkownicy**, a następnie kliknij łącze **Przejdź do modułu Email Security** w prawym górnym rogu.

Dodatkowe informacje na temat funkcji Advanced Email Security można znaleźć na karcie produktu Advanced Email Security.

Instrukcje konfiguracji można znaleźć w sekcji Advanced Email Security z rozwiązaniem Perception Point.

Ochrona danych pakietu Google Workspace

Uwaga
Ta funkcja nie jest dostępna w przypadku dzierżawców w trybie zgodności. Aby uzyskać więcej informacji, zobacz sekcję "Tryb zgodności" (s. 1180).

Co oznacza ochrona danych pakietu Google Workspace?

- Tworzenie kopii zapasowych i odzyskiwanie danych użytkowników pakietu Google Workspace (skrzynek pocztowych Gmail, kalendarzy, kontaktów, plików z Dysku Google) oraz Dysków udostępnionych Google Workspace z chmury do chmury.
- Odzyskiwanie granularne wiadomości e-mail, plików, kontaktów i innych elementów.
- Obsługa kilku organizacji Google Workspace i odzyskiwania między organizacjami.
- Opcjonalna notaryzacja plików z kopii zapasowej za pomocą bazy danych łańcucha bloków Ethereum. W przypadku włączenia tej opcji można udowodnić, że plik jest autentyczny i niezmieniony od chwili uwzględnienia w kopii zapasowej.
- Opcjonalne wyszukiwanie pełnotekstowe. W przypadku włączenia tej funkcji można wyszukiwać wiadomości e-mail według ich zawartości.
- Można chronić do 5000 elementów (skrzynek pocztowych, Dysków Google i Dysków udostępnionych) na firmę bez spadku wydajności.
- Dane zapisywane w kopii zapasowej są automatycznie kompresowane i zajmują mniej miejsca w lokalizacji kopii zapasowych niż w pierwotnej lokalizacji. Poziom kompresji w przypadku kopii

 © Acronis International GmbH, 2003-2024

zapasowych z chmury do chmury jest stały i odpowiada poziomowi kompresji **Normalny** stosowanemu w przypadku innych kopii zapasowych. Dodatkowe informacje na temat tych poziomów można znaleźć w sekcji "Stopień kompresji" (s. 492).

Wymagane prawa użytkownika

W programie Cyber Protection

W programie Cyber Protection trzeba być administratorem firmy działającym na poziomie dzierżawcy-klienta. Administratorzy firm działający na poziomie jednostek, administratorzy jednostek i użytkownicy nie mogą tworzyć kopii zapasowych ani odzyskiwać danych pakietu Google Workspace.

W pakiecie Google Workspace

Aby dodać organizację Google Workspace do usługi Cyber Protection, trzeba się zalogować jako superadministrator z włączonym dostępem do interfejsów API (**Security** [Zabezpieczenia] > **API reference** [Wykaz interfejsów API] > **Enable API access** [Włącz dostęp do interfejsów API] w konsoli administracyjnej Google).

Hasło superadministratora nie jest nigdzie przechowywane i nie jest używane do tworzenia kopii zapasowych i odzyskiwania danych. Zmiana tego hasła w pakiecie Google Workspace nie ma wpływu na działanie usługi Cyber Protection.

Jeśli superadministrator, który dodał organizację Google Workspace, zostanie usunięty z pakietu Google Workspace lub otrzyma rolę z mniejszymi uprawnieniami, kopie zapasowe zakończą się niepowodzeniem z komunikatem o błędzie, np. „Odmowa dostępu”. W takim przypadku należy powtórzyć procedurę opisaną w sekcji "Dodawanie organizacji Google Workspace" (s. 688) i podać prawidłowe poświadczenia superadministratora. Aby uniknąć takiej sytuacji, warto utworzyć specjalnego superadministratora do celów tworzenia kopii zapasowych i odzyskiwania.

Informacje o harmonogramie tworzenia kopii zapasowych

Ponieważ agent w chmurze obsługuje wielu klientów, sam ustala czas rozpoczęcia wykonywania poszczególnych planów ochrony, aby uzyskać równomierne obciążenie w ciągu dnia i taką samą jakość usług dla każdego klienta.

Każdy plan ochrony jest wykonywany codziennie o tej samej porze.

Domyślnie jest ustawiona opcja **Raz dziennie**. Pakiet Zaawansowane tworzenie kopii zapasowych umożliwia zaplanowanie do sześciu operacji tworzenia kopii zapasowych dziennie. Operacje tworzenia kopii zapasowych są uruchamiane w przybliżonych odstępach, które zależą od bieżącego obciążenia agenta w chmurze, obsługującego wielu klientów w centrum danych. Zapewnia to równomierne obciążenie w ciągu dnia i jednakową jakość obsługi wszystkich klientów.

© Acronis International GmbH, 2003-2024

Ograniczenia

- W konsoli są widoczni tylko ci użytkownicy, którzy mają przypisane licencję i skrzynkę pocztową usługi Google Workspace lub Dysk Google.
- Dokumenty w macierzystych formatach Google są zapisywane w kopii zapasowej jako zwykłe dokumenty pakietu Office i wyświetlane w konsoli Cyber Protect z innym rozszerzeniem, na przykład .docx lub .pptx. Podczas odzyskiwania są konwertowane z powrotem na pierwotny format.
- Maksymalnie 10 ręcznie wykonywanych operacji tworzenia kopii zapasowej w ciągu godziny.
- Maksymalnie 10 jednoczesnych operacji odzyskiwania (ta liczba obejmuje odzyskiwanie danych zarówno pakietu Microsoft 365, jak i pakietu Google Workspace).
- Nie można równolegle odzyskiwać elementów z różnych punktów odzyskiwania, nawet jeśli da się wybrać takie elementy z wyników wyszukiwania.
- Kopie zapasowe usuniętych kont użytkowników rozwiązania Google Workspace nie są automatycznie usuwane z chmury. W przypadku tych kopii zapasowych naliczane są opłaty za zajmowane przez nie miejsce w pamięci masowej.
- Do danego obciążenia nie można zastosować więcej niż jednego indywidualnego planu tworzenia kopii zapasowych.
- Jeśli do tego samego obciążenia zastosowano indywidualny plan tworzenia kopii zapasowych i grupowy plan tworzenia kopii zapasowych, ustawienia planu indywidualnego mają pierwszeństwo.

Prowadzenie dziennika

Niektóre czynności dotyczące zasobów międzychmurowych, takie jak przeglądanie zawartości wiadomości e-mail w kopiach zapasowych, pobieranie załączników lub plików, odzyskiwanie wiadomości e-mail do skrzynek pocztowych innych niż pierwotne lub wysyłanie zasobów jako wiadomości e-mail, mogą naruszać prywatność użytkowników. Czynności te są rejestrowane w sekcji **Monitorowanie** > **Dziennik inspekcji** w portalu zarządzania.

Dodawanie organizacji Google Workspace

Aby dodać organizację Google Workspace do usługi Cyber Protection, trzeba mieć specjalny osobisty projekt Google Cloud. Dodatkowe informacje na temat tworzenia i konfigurowania takiego projektu można znaleźć w sekcji "Tworzenie osobistego projektu Google Cloud" (s. 689).

Aby dodać organizację Google Workspace przy użyciu specjalnego osobistego projektu Google Cloud

1. Zaloguj się do konsoli Cyber Protect jako administrator firmy.
2. Kliknij **Urządzenia** > **Dodaj** > **Google Workspace**.

© Acronis International GmbH, 2003-2024

3. Wprowadź adres e-mail superadministratora konta Google Workspace.
   W przypadku tej procedury nie ma znaczenia, czy dla konta e-mail superadministratora została włączona weryfikacja dwuetapowa.
4. Znajdź plik JSON z kluczem prywatnym konta usługi, który został utworzony w projekcie Google Cloud.
   Możesz też wkleić zawartość pliku jako tekst.

5. Kliknij **Potwierdź**.

W wyniku tych działań organizacja Google Workspace pojawi się na karcie **Urządzenia** w konsoli Cyber Protect.

Przydatne porady

- Po dodaniu organizacji Google Workspace dane użytkownika i Dyski współdzielone — zarówno te z domeny głównej, jak i ewentualnych domen drugorzędnych — zostaną skopiowane. Zasoby uwzględnione w kopii zapasowej zostaną wyświetlone na jednej liście, tj. nie będą pogrupowane według domen.
- Agent w chmurze dokonuje synchronizacji z pakietem Google Workspace co 24 godziny, zaczynając od momentu dodania organizacji do usługi Cyber Protection. Jeśli dodasz lub usuniesz użytkownika bądź dysk współdzielony, zmiany nie będą od razu widoczne w konsoli Cyber Protect. Aby niezwłocznie zsynchronizować zmianę, wybierz organizację na stronie **Google Workspace**, a następnie kliknij **Odśwież**.
  Dodatkowe informacje na temat synchronizowania zasobów organizacji Google Workspace i konsoli Cyber Protect można znaleźć w sekcji "Wykrywanie zasobów z usługi Google Workspace" (s. 693).
- Jeśli plan ochrony został zastosowany do grup **Wszyscy użytkownicy** lub **Wszystkie dyski współdzielone**, nowo dodane elementy zostaną uwzględnione w kopii zapasowej dopiero po synchronizacji.
- Zgodnie z zasadami firmy Google użytkownik lub Dysk współdzielony usunięty z graficznego interfejsu użytkownika pakietu Google Workspace pozostaje dostępny za pośrednictwem interfejsu API jeszcze przez kilka dni. W tym okresie usunięty element jest nieaktywny (wyszarzony) w konsoli Cyber Protect i nie jest uwzględniany w kopiach zapasowych. Gdy usunięty element przestanie być dostępny za pośrednictwem interfejsu API, przestanie też być widoczny w konsoli Cyber Protect. Jego kopie zapasowe (jeśli jakieś istnieją) można znaleźć w obszarze **Magazyn kopii zapasowych** > **Kopie zapasowe aplikacji w chmurze**.

Tworzenie osobistego projektu Google Cloud

Aby dodać organizację Google Workspace do usługi Cyber Protection przy użyciu specjalnego projektu Google Cloud:

1. Utwórz nowy projekt Google Cloud.
2. Włącz wymagane interfejsy API dla tego projektu.

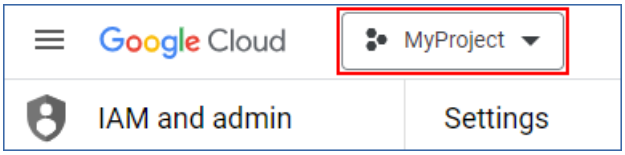
© Acronis International GmbH, 2003-2024

3. Skonfiguruj poświadczenia dla tego projektu:
   a. Skonfiguruj ekran akceptacji OAuth.
   b. Utwórz i skonfiguruj konto usługi Cyber Protection.
4. Przyznaj nowemu projektowi dostęp do swojego konta Google Workspace.

Uwaga
Ten temat zawiera opis interfejsu użytkownika oprogramowania innej firmy, który może ulec zmianie bez uprzedzenia.

Aby utworzyć nowy projekt Google Cloud

1. Zaloguj się do Google Cloud Platform (console.cloud.google.com) jako superadministrator.
2. W konsoli Google Cloud Platform kliknij narzędzie wyboru projektów w lewym górnym rogu.



3. Na wyświetlonym ekranie wybierz organizację, a następnie kliknij **Nowy projekt**.

4. Określ nazwę nowego projektu.
5. Kliknij **Utwórz**.

W wyniku tych działań zostanie utworzony nowy projekt Google Cloud.

Aby włączyć wymagane interfejsy API dla tego projektu

1. W konsoli Google Cloud Platform wybierz swój nowy projekt.
2. W menu nawigacyjnym wybierz **Interfejsy API i usługi** > **Włączone interfejsy API i usługi**.
3. Wyłącz po kolei wszystkie interfejsy API, które są domyślnie włączone w projekcie:
   a. Przewiń stronę **Włączone interfejsy API i usługi** w dół i kliknij nazwę włączonego interfejsu API.
   Zostanie otwarta strona **Szczegóły interfejsów API / usług** z informacjami dotyczącymi wybranego interfejsu API.
   b. Kliknij **Wyłącz API**, a następnie potwierdź wybór, klikając **Wyłącz**.
   c. [Jeśli pojawi się monit] Potwierdź wybór, klikając **Potwierdź**.
   d. Wróć do obszaru **Interfejsy API i usługi** > **Włączone interfejsy API i usługi** i wyłącz kolejny interfejs API.
4. W menu nawigacyjnym wybierz **Interfejsy API i usługi** > **Biblioteka**.
5. W bibliotece interfejsów API włącz po kolei następujące interfejsy API:

© Acronis International GmbH, 2003-2024

- Admin SDK API
- Gmail API
- Google Calendar API
- Google Drive API
- Google People API

Aby znaleźć wymagane interfejsy API, skorzystaj z paska wyszukiwania. W celu włączenia interfejsu API kliknij jego nazwę, a następnie kliknij **Włącz**. Aby wyszukać kolejny interfejs API, wróć do biblioteki interfejsów API, wybierając w menu nawigacyjnym **Interfejsy API i usługi** > **Biblioteka**.

Aby skonfigurować ekran akceptacji OAuth

1. W menu nawigacyjnym Google Cloud Platform wybierz **Interfejsy API i usługi** > **Ekran zgody na uwierzytelnianie OAuth**.
2. W otwartym oknie zaznacz typ użytkownika **Wewnętrzny** i kliknij **Utwórz**.
3. W polu **Nazwa aplikacji** podaj nazwę aplikacji.
4. W polu **Adres e-mail dla użytkowników potrzebujących pomocy** wprowadź adres e-mail superadministratora.
5. W polu **Dane kontaktowe dewelopera** wprowadź adres e-mail superadministratora.
6. Zostaw pozostałe pola puste i kliknij **Zapisz i kontynuuj**.
7. Na stronie **Zakresy** kliknij **Zapisz i kontynuuj** bez jakichkolwiek zmian.
8. Na stronie **Podsumowanie** zweryfikuj swoje ustawienia i kliknij **Powrót do panelu**.

Aby utworzyć i skonfigurować konto usługi Cyber Protection

1. W menu nawigacyjnym Google Cloud Platform wybierz **Administracja** > **Konta usługi**.
2. Kliknij **Utwórz konto usługi**.
3. Określ nazwę konta usługi.
4. [Opcjonalnie] Dodaj opis konta usługi.
5. Kliknij **Utwórz i kontynuuj**.
6. W ramach kroków **Przyznaj temu kontu usługi dostęp do projektu** i **Przyznaj użytkownikom dostęp do tego konta usługi** nie wprowadzaj żadnych zmian.
7. Kliknij **Gotowe**.
   Zostanie otwarta strona **Konta usługi**.
8. Na stronie **Konta usługi** zaznacz nowe konto usługi, a następnie w obszarze **Działania** kliknij **Zarządzaj kluczami**.
9. Na karcie **Klucze** kliknij **Dodaj klucz** > **Utwórz nowy klucz** i wybierz typ klucza **JSON**.
10. Kliknij **Utwórz**.

© Acronis International GmbH, 2003-2024

W wyniku tych działań na Twój komputer zostanie automatycznie pobrany plik JSON z kluczem prywatnym konta usługi. Zapisz ten plik w bezpiecznym miejscu, ponieważ będzie on potrzebny do dodania organizacji Google Workspace do usługi Cyber Protection.

Aby przyznać nowemu projektowi dostęp do swojego konta Google Workspace

1. W menu nawigacyjnym Google Cloud Platform wybierz **IAM i administracja** > **Konta usługi**.
2. Na liście znajdź utworzone konto usługi, a następnie skopiuj identyfikator klienta wyświetlany w kolumnie **Identyfikator klienta OAuth 2.0**.
3. Zaloguj się do konsoli administracyjnej Google (admin.google.com) jako superadministrator.
4. W menu nawigacyjnym wybierz **Zabezpieczenia** > **Kontrola dostępu i danych** > **Kontrola nad interfejsami API**.
5. Przewiń stronę **Kontrola nad dostępem do aplikacji** w dół i w obszarze **Przekazywanie dostępu w całej domenie** kliknij **Zarządzaj przekazywaniem dostępu w całej domenie**. Zostanie otwarta strona **Przekazywanie dostępu w całej domenie**.
6. Na stronie **Przekazywanie dostępu w całej domenie** kliknij **Dodaj nowy**.
   Zostanie otwarte okno **Dodaj nowy identyfikator klienta**.
7. W polu **Identyfikator klienta** wprowadź identyfikator klienta konta usługi.
8. Skopiuj poniższą listę zakresów rozdzielonych przecinkami i wklej ją w polu **Zakresy uwierzytelniania OAuth**:

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googlea
   pis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,
   https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleap
   is.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   Możesz też dodać zakresy — po jednym w każdym wierszu:
   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/drive
   - https://www.googleapis.com/auth/gmail.modify
9. Kliknij **Autoryzuj**.

W wyniku tych działań Twój nowy projekt Google Cloud zyska możliwość dostępu do danych na Twoim koncie Google Workspace. Aby utworzyć kopię zapasową tych danych, trzeba powiązać ten projekt z usługą Cyber Protection. Dodatkowe informacje o tym, jak to zrobić, można znaleźć w sekcji "Aby dodać organizację Google Workspace przy użyciu specjalnego osobistego projektu Google Cloud" (s. 688).

© Acronis International GmbH, 2003-2024

Jeśli zechcesz odwołać dostęp projektu Google Cloud do konta Google Workspace i odpowiednio dostęp do usługi Cyber Protection, usuń klienta interfejsu API używanego przez ten projekt.

Aby odwołać dostęp projektu do Twojego konta Google Workspace

1. W konsoli administracyjnej Google (admin.google.com) zaloguj się jako superadministrator.
2. W menu nawigacyjnym wybierz **Zabezpieczenia** > **Kontrola dostępu i danych** > **Kontrola nad interfejsami API**.
3. Przewiń stronę **Kontrola nad dostępem do aplikacji** w dół i w obszarze **Przekazywanie dostępu w całej domenie** kliknij **Zarządzaj przekazywaniem dostępu w całej domenie**. Zostanie otwarta strona **Przekazywanie dostępu w całej domenie**.
4. Na stronie **Przekazywanie dostępu w całej domenie** wybierz klienta interfejsu API, którego używa projekt, i kliknij **Usuń**.
   W wyniku tych działań Twój projekt Google Cloud i usługa Cyber Protection nie będą już mogły uzyskiwać dostępu do Twojego konta Google Workspace ani tworzyć kopii zapasowych znajdujących się na nim danych.

Wykrywanie zasobów z usługi Google Workspace

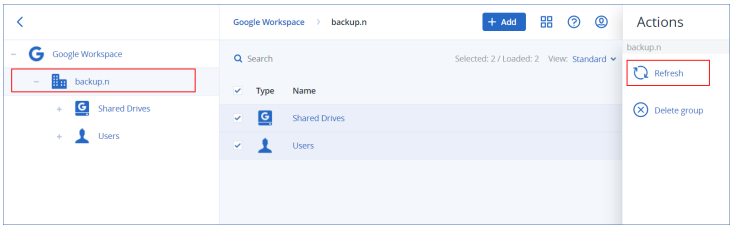
W przypadku dodania organizacji Google Workspace do rozwiązania Cyber Protection zasoby z tej organizacji, na przykład skrzynki pocztowe i Dyski Google, są synchronizowane z konsolą Cyber Protect. Operacja ta jest nazywana wykrywaniem i jest rejestrowana w sekcji **Monitorowanie** > **Działania**.

Po zakończeniu operacji wykrywania zasoby z organizacji Google Workspace będą widoczne na karcie **Urządzenia** > **Google Workspace** w konsoli Cyber Protect i będzie można stosować do nich plany tworzenia kopii zapasowych.

Operacja wykrywania jest wykonywana automatycznie raz dziennie, aby zapewnić aktualność listy zasobów w konsoli Cyber Protect. Listę tę można też synchronizować na żądanie przez ręczne uruchomienie operacji wykrywania.

Aby ręcznie uruchomić operację wykrywania

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Google Workspace**.
2. Zaznacz organizację Google Workspace, a następnie w panelu **Czynności** kliknij **Odśwież**.



© Acronis International GmbH, 2003-2024

Uwaga
Operację wykrywania można uruchomić ręcznie do 10 razy na godzinę. Po osiągnięciu tej liczby ustawienie limitu dozwolonych uruchomień zostaje ograniczone do jednego razu na godzinę, a następnie co godzinę udostępniana jest dodatkowa operacja, aż do ponownego osiągnięcia limitu 10 operacji na godzinę.

Ustawianie częstotliwości tworzenia kopii zapasowych danych Google Workspace

Domyślnie kopie zapasowe danych Google Workspace są tworzone raz dziennie i nie ma dodatkowych opcji planowania.

Jeśli w ramach dzierżawcy jest włączony pakiet Zaawansowane tworzenie kopii zapasowych, można skonfigurować częstsze tworzenie kopii zapasowych. Można wybrać liczbę kopii zapasowych dziennie, ale nie można skonfigurować godziny rozpoczęcia operacji tworzenia kopii zapasowej. Operacje tworzenia kopii zapasowych są uruchamiane automatycznie w przybliżonych odstępach, które zależą od bieżącego obciążenia agenta w chmurze, obsługującego wielu klientów w centrum danych. Zapewnia to równomierne obciążenie w ciągu dnia i jednakową jakość obsługi wszystkich klientów.

Dostępne są następujące opcje.

Opcje planowania	Przybliżony odstęp między operacjami tworzenia kopii zapasowych
Raz dziennie	24 godz.
2 razy dziennie (domyślnie)	12 godzin
3 razy dziennie	8 godzin
6 razy dziennie	4 godziny

Uwaga
W zależności od obciążenia agenta w chmurze i ewentualnego ograniczenia po stronie Google Workspace tworzenie kopii zapasowej może się rozpocząć później niż zaplanowano lub potrwać dłużej. Jeśli tworzenie kopii zapasowej trwa dłużej niż średni odstęp czasowy między dwiema operacjami tworzenia kopii zapasowych, następna kopia zapasowa zostanie przełożona, co może skutkować mniejszą liczbą kopii zapasowych dziennie niż wybrano. Na przykład, mogą zostać utworzone tylko dwie kopie zapasowe dziennie — nawet jeśli wybrano sześć kopii dziennie.

© Acronis International GmbH, 2003-2024

Ochrona danych rozwiązania Gmail

Jakie elementy można uwzględnić w kopii zapasowej?

W kopii zapasowej można uwzględnić skrzynki pocztowe użytkowników rozwiązania Gmail. Kopia zapasowa skrzynek pocztowych obejmuje również dane kalendarza i dane kontaktów. Opcjonalnie można wybrać utworzenie kopii zapasowej archiwalnych kalendarzy współdzielonych.

Podczas tworzenia kopii zapasowej są *pomijane* następujące elementy:

- Kalendarze z **urodzinami**, **przypomnieniami** i **zadaniami**
- Foldery załączone do wydarzeń w kalendarzu
- Folder **Directory** w obszarze Kontakty

Z powodu ograniczeń interfejsu API Kalendarza Google są *pomijane* następujące elementy z Kalendarza:

- Przydziały czasu na spotkania
- Pole konferencji w wydarzeniu
- Ustawienie kalendarza **Powiadomienia o wydarzeniach całodniowych**
- Ustawienie kalendarza **Automatycznie przyjmuj zaproszenia** (w kalendarzach dotyczących sal i przestrzeni wspólnych)

Z powodu ograniczeń interfejsu API Kontaktów Google są *pomijane* następujące elementy z obszaru Osoby:

- Folder **Inne kontakty**
- Zewnętrzne profile kontaktu (**Profil Directory**, **Profil Google**)
- Pole kontaktu **Zarejestruj jako**

Jakie elementy można odzyskać?

Z kopii zapasowej skrzynek pocztowych można odzyskać następujące elementy:

- Skrzynki pocztowe
- Foldery poczty e-mail (zgodnie z terminologią Google: „etykiety”. **Etykiety** są określane w programie do tworzenia kopii zapasowych jako foldery — w celu zachowania spójności z innymi formami prezentacji danych).
- Wiadomości e-mail
- Zdarzenia kalendarza
- Kontakty

Możesz użyć wyszukiwania w celu odnalezienia elementów w kopii zapasowej.

© Acronis International GmbH, 2003-2024

Odzyskując skrzynki pocztowe i elementy skrzynek pocztowych, możesz wybrać, czy chcesz nadpisać elementy w lokalizacji docelowej.

Ograniczenia

- Nie można odzyskać zdjęć kontaktów.
- Z powodu ograniczeń interfejsu API Kalendarza Google element kalendarza **Poza biurem** jest odzyskiwany jako zwykłe wydarzenie w kalendarzu.

Wybieranie skrzynek pocztowych Gmail

Wybierz skrzynki pocztowe zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać skrzynki pocztowe Gmail

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, w której przypadku chcesz utworzyć kopię zapasową danych użytkowników. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby tworzyć kopie zapasowe skrzynek pocztowych wszystkich użytkowników (w tym skrzynek pocztowych, które zostaną utworzone w przyszłości), rozwiń węzeł **Użytkownicy**, wybierz **Wszyscy użytkownicy**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby tworzyć kopie zapasowe skrzynek pocztowych wybranych użytkowników, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, następnie wybierz użytkowników, dla których chcesz wykonać kopię zapasową skrzynek pocztowych, po czym kliknij **Kopia zapasowa**.
4. W panelu planu ochrony:
   - Upewnij się, że w obszarze **Elementy uwzględniane w kopii zapasowej** jest zaznaczona pozycja **Gmail**.
   - Jeśli chcesz utworzyć kopię zapasową kalendarzy udostępnionych wybranym użytkownikom, włącz przełącznik **Uwzględnij kalendarze udostępnione**.
   - Zdecyduj, czy potrzebujesz obsługi wyszukiwania pełnotekstowego w wiadomościach e-mail uwzględnionych w kopii zapasowej. Aby uzyskać dostęp do tej opcji, kliknij ikonę koła zębatego > **Opcje tworzenia kopii zapasowych** > **Wyszukiwanie pełnotekstowe**.

Odzyskiwanie skrzynek pocztowych i elementów skrzynek pocztowych

Odzyskiwanie skrzynek pocztowych

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.

© Acronis International GmbH, 2003-2024

3. Rozwiń węzeł **Użytkownicy**, wybierz **Wszyscy użytkownicy**, wskaż użytkownika, którego skrzynkę pocztową chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
   Jeśli użytkownik został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
   Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

   Uwaga
   Aby wyświetlić wyłącznie punkty odzyskiwania zawierające skrzynki pocztowe, wybierz **Gmail** w polu **Filtruj według zawartości**.

5. Kliknij **Odzyskaj** > **Cała skrzynka pocztowa**.
6. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, kliknij **Organizacja Google Workspace**, aby wyświetlić, zmienić lub określić organizację docelową.
   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wybrać nową organizację docelową spośród dostępnych zarejestrowanych organizacji.
7. W polu **Odzyskaj do skrzynki pocztowej** wyświetl, zmień lub określ docelową skrzynkę pocztową.
   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelową skrzynkę pocztową.
   Podczas odzyskiwania nie można utworzyć nowej docelowej skrzynki pocztowej. Aby odzyskać skrzynkę pocztową do nowej skrzynki, należy najpierw utworzyć docelową skrzynkę pocztową w wybranej organizacji Google Workspace, a następnie pozwolić agentowi w chmurze na zsynchronizowanie zmiany. Agent w chmurze automatycznie przeprowadza synchronizację ze środowiskiem Google Workspace co 24 godziny. Aby niezwłocznie zsynchronizować zmianę, w konsoli Cyber Protect wybierz organizację na stronie **Google Workspace**, a następnie kliknij **Odśwież**.
8. Kliknij **Rozpocznij odzyskiwanie**.
9. Wybierz jedną z następujących opcji zastępowania:
   - **Zastąp istniejące elementy**
   - **Nie zastępuj istniejących elementów**
10. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Odzyskiwanie elementów skrzynki pocztowej

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.

© Acronis International GmbH, 2003-2024

3. Rozwiń węzeł **Użytkownicy**, wybierz **Wszyscy użytkownicy**, wskaż użytkownika, którego skrzynka pocztowa pierwotnie zawierała elementy, które chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

   Jeśli użytkownik został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

   Użytkowników i grupy można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

   Uwaga
   Aby wyświetlić wyłącznie punkty odzyskiwania zawierające skrzynki pocztowe, wybierz **Gmail** w polu **Filtruj według zawartości**.
5. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
6. Przejdź do odpowiedniego folderu. Jeśli kopia zapasowa nie jest zaszyfrowana, możesz skorzystać z funkcji wyszukiwania, aby uzyskać listę potrzebnych elementów.

   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.
   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata, daty, nazwy załącznika i zawartości wiadomości.

     Jeśli zdecydujesz się na wyszukiwanie według daty, możesz wybrać datę początkową lub końcową (obie włącznie) albo obie te daty, aby wyszukiwać w zakresie czasu.

     Wyszukiwanie według nazwy załącznika lub w treści wiadomości daje wyniki tylko wtedy, gdy podczas operacji tworzenia kopii zapasowej włączono opcję **Wyszukiwanie pełnotekstowe**. Jako dodatkowy parametr można określić język szukanego fragmentu wiadomości.
   - Zdarzenia: wyszukiwanie według tematu i daty.
   - Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.
7. Wybierz elementy, które chcesz odzyskać. Aby mieć możliwość wybrania folderów, kliknij ikonę „Odzyskaj foldery”:

   Możesz również wykonać dowolną z następujących czynności:
   - Po wybraniu elementu kliknij **Pokaż zawartość**, aby zobaczyć jego zawartość, w tym załączniki. Kliknij nazwę załączonego pliku, aby go pobrać.
   - Tylko w sytuacji, gdy kopia zapasowa nie jest zaszyfrowana, a w wynikach wyszukiwania wybrano jeden element: kliknij **Pokaż wersje**, aby wybrać wersję elementu do odzyskania. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.
8. Kliknij **Odzyskaj**.
9. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, kliknij **Organizacja Google Workspace**, aby wyświetlić, zmienić lub określić organizację docelową.

© Acronis International GmbH, 2003-2024

Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wybrać nową organizację docelową spośród dostępnych zarejestrowanych organizacji.

10. W polu **Odzyskaj do skrzynki pocztowej** wyświetl, zmień lub określ docelową skrzynkę pocztową.

    Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelową skrzynkę pocztową.
11. W polu **Ścieżka** wyświetl lub zmień folder docelowy w docelowej skrzynce pocztowej. Domyślnie wybrany jest pierwotny folder.
12. Kliknij **Rozpocznij odzyskiwanie**.
13. Wybierz jedną z następujących opcji zastępowania:
    - **Zastąp istniejące elementy**
    - **Nie zastępuj istniejących elementów**
14. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Ochrona plików z Dysku Google

Jakie elementy można uwzględnić w kopii zapasowej?

Można utworzyć kopię zapasową całego Dysku Google lub znajdujących się w nim poszczególnych plików i folderów. Pliki są zapisywane razem z ich uprawnieniami udostępnienia.

Ważne
W kopii zapasowej nie są uwzględniane następujące elementy:

- Folder **Udostępnione mi**
- Folder **Komputery** (utworzony przez klienta Kopie zapasowe i synchronizacja)

Ograniczenia

Spośród formatów plików oprogramowania Google podczas operacji tworzenia kopii zapasowych w pełni są obsługiwane tylko dokumenty Google, arkusze Google i slajdy prezentacji Google. Inne formaty oprogramowania Google mogą nie być w pełni obsługiwane lub mogą wcale nie być obsługiwane. Na przykład pliki oprogramowania Rysunki Google są odzyskiwane jako pliki `.svg`, pliki oprogramowania Witryny Google — jako pliki `.txt`, pliki oprogramowania Google Jamboard — jako pliki `.pdf`, a pliki oprogramowania Moje Mapy Google są pomijane podczas tworzenia kopii zapasowej.

Uwaga
Formaty plików, które nie są specyficzne dla oprogramowania Google — takie jak `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png` czy `.zip` — są w pełni obsługiwane podczas tworzenia kopii zapasowej i odzyskiwania.

© Acronis International GmbH, 2003-2024

Jakie elementy można odzyskać?

Można odzyskać cały Dysk Google lub dowolny plik bądź folder, który został uwzględniony w kopii zapasowej.

Można wybrać opcję odzyskania uprawnień udostępnienia lub dziedziczenia przez pliki uprawnień z folderu, do którego są odzyskiwane.

Ograniczenia

- Komentarze zamieszczone w plikach nie są odzyskiwane.
- Nie można odzyskać łączy umożliwiających udostępnianie plików i folderów.
- **Ustawienia właściciela** tylko do odczytu skonfigurowane w przypadku plików udostępnionych (**Zablokuj edytorom możliwość wprowadzania zmian dostępu i dodawania nowych osób** i **Wyłącz pobieranie, drukowanie i kopiowanie dla komentujących i przeglądających**) nie mogą zostać zmienione podczas odzyskiwania.
- Jeśli w przypadku folderu udostępnionego jest włączona opcja **Zablokuj edytorom możliwość wprowadzania zmian dostępu i dodawania nowych osób**, nie można zmienić praw własności tego folderu podczas odzyskiwania. To ustawienie uniemożliwia interfejsowi API Dysku Google wyświetlanie uprawnień do folderów. Prawa własności plików w folderze są prawidłowo odzyskiwane.

Wybieranie plików z Dysku Google

Wybierz pliki zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać pliki z Dysku Google

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, w której przypadku chcesz utworzyć kopię zapasową danych użytkowników. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby tworzyć kopie zapasowe plików wszystkich użytkowników (w tym użytkowników, którzy zostaną utworzeni w przyszłości), rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby tworzyć kopie zapasowe plików wybranych użytkowników, rozwiń węzeł **Użytkownicy**, wybierz opcję **Wszyscy użytkownicy**, następnie wybierz użytkowników, dla których chcesz wykonać kopię zapasową skrzynek pocztowych, po czym kliknij **Kopia zapasowa**.
4. W panelu planu ochrony:
   - Upewnij się, że w obszarze **Elementy uwzględniane w kopii zapasowej** jest zaznaczona pozycja **Dysk Google**.

© Acronis International GmbH, 2003-2024

- W obszarze **Elementy uwzględniane w kopii zapasowej** wykonaj jedną z następujących czynności:
  - Zachowaj ustawienie domyślne **[Wszystkie]** (wszystkie pliki).
  - Określ pliki i foldery do uwzględnienia w kopii zapasowej, dodając ich nazwy lub ścieżki.
    Można używać symboli wieloznacznych (*, ** i ?). Aby uzyskać więcej informacji na temat określania ścieżek i stosowania symboli wieloznacznych, zobacz „Filtry plików".
  - Określ pliki i foldery do uwzględnienia w kopii zapasowej, przeglądając je.
    Łącze **Przeglądaj** jest dostępne tylko w przypadku tworzenia planu ochrony dla jednego użytkownika.
- [Opcjonalnie] W obszarze **Elementy uwzględniane w kopii zapasowej** kliknij **Pokaż wykluczenia**, aby określić pliki i foldery, które mają zostać pominięte w procesie tworzenia kopii zapasowej.
  Wykluczenia plików mają wyższy priorytet niż wybór plików, tj. w przypadku wskazania tego samego pliku w obu polach zostanie on pominięty podczas tworzenia kopii zapasowej.
- Aby włączyć notaryzację wszystkich plików wybranych do uwzględnienia kopii zapasowej, włącz przełącznik **Notaryzacja**. Więcej informacji o notaryzacji można znaleźć w sekcji „Notaryzacja".

Odzyskiwanie Dysku Google i plików z Dysku Google

Odzyskiwanie całego Dysku Google

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Użytkownicy**, wybierz **Wszyscy użytkownicy**, wskaż użytkownika, którego Dysk Google chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
   Jeśli użytkownik został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
   Użytkowników można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

   Uwaga
   Aby wyświetlić wyłącznie punkty odzyskiwania zawierające pliki z Dysku Google, wybierz opcję **Dysk Google** w polu **Filtruj według zawartości**.

5. Kliknij **Odzyskaj** > **Cały dysk**.
6. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, kliknij **Organizacja Google Workspace**, aby wyświetlić, zmienić lub określić organizację docelową.
   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wybrać nową organizację docelową spośród dostępnych zarejestrowanych organizacji.

© Acronis International GmbH, 2003-2024

7. W polu **Odzyskaj na dysk** wyświetl, zmień lub określ użytkownika docelowego lub docelowy Dysk udostępniony.

   Domyślnie jest wybrany pierwotny użytkownik. Jeśli użytkownik nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić użytkownika docelowego lub docelowy Dysk udostępniony.

   Jeśli kopia zapasowa zawiera udostępnione pliki, zostaną one odzyskane do folderu głównego dysku docelowego.
8. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania plików.
9. Kliknij **Rozpocznij odzyskiwanie**.
10. Wybierz jedną z następujących opcji zastępowania:

Opcja	Opis
Zastąp istniejący plik, jeśli jest starszy	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie jak plik źródłowy, ale starszy od niego, plik źródłowy zostanie zapisany w lokalizacji docelowej, zastępując starszą wersję.
Zastąp istniejące pliki	Wszystkie pliki w lokalizacji docelowej zostaną zastąpione, niezależnie od daty ich ostatniej modyfikacji.
Nie zastępuj istniejących plików	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie, nie zostaną do niego zastosowane żadne zmiany, a plik źródłowy nie zostanie zapisany w lokalizacji docelowej.

11. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Odzyskiwanie plików z Dysku Google

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Użytkownicy**, wybierz **Wszyscy użytkownicy**, wskaż użytkownika, którego pliki z Dysku Google chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

   Jeśli użytkownik został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

   Użytkowników można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
4. Wybierz punkt odzyskiwania.

   Uwaga
   Aby wyświetlić wyłącznie punkty odzyskiwania zawierające pliki z Dysku Google, wybierz opcję **Dysk Google** w polu **Filtruj według zawartości**.

5. Kliknij **Odzyskaj** > **Pliki/foldery**.
6. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych plików i folderów.

© Acronis International GmbH, 2003-2024

7. Wybierz pliki, które chcesz odzyskać.

   Jeśli kopia zapasowa nie jest zaszyfrowana i wybrano jeden plik, możesz kliknąć **Pokaż wersje**, aby wybrać wersję pliku do odzyskania. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.
8. Jeśli chcesz pobrać plik, zaznacz go, kliknij **Pobierz**, wybierz lokalizację, w której ma zostać zapisany plik, i kliknij **Zapisz**. W przeciwnym razie pomiń ten krok.
9. Kliknij **Odzyskaj**.
10. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, kliknij **Organizacja Google Workspace**, aby wyświetlić, zmienić lub określić organizację docelową.

    Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wybrać nową organizację docelową spośród dostępnych zarejestrowanych organizacji.
11. W polu **Odzyskaj na dysk** wyświetl, zmień lub określ użytkownika docelowego lub docelowy Dysk udostępniony.

    Domyślnie jest wybrany pierwotny użytkownik. Jeśli użytkownik nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelowego użytkownika lub docelowy Dysk udostępniony.
12. W polu **Ścieżka** wyświetl lub zmień folder docelowy w Dysku Google docelowego użytkownika lub docelowym Dysku udostępnionym. Domyślnie jest wybrana pierwotna lokalizacja.
13. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania plików.
14. Kliknij **Rozpocznij odzyskiwanie**.
15. Wybierz jedną z następujących opcji zastępowania plików:

Opcja	Opis
Zastąp istniejący plik, jeśli jest starszy	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie jak plik źródłowy, ale starszy od niego, plik źródłowy zostanie zapisany w lokalizacji docelowej, zastępując starszą wersję.
Zastąp istniejące pliki	Wszystkie pliki w lokalizacji docelowej zostaną zastąpione, niezależnie od daty ich ostatniej modyfikacji.
Nie zastępuj istniejących plików	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie, nie zostaną do niego zastosowane żadne zmiany, a plik źródłowy nie zostanie zapisany w lokalizacji docelowej.

16. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Ochrona plików z Dysku udostępnionego

Jakie elementy można uwzględnić w kopii zapasowej?

Można utworzyć kopię zapasową całego Dysku udostępnionego lub znajdujących się w nim poszczególnych plików i folderów. Pliki są zapisywane razem z ich uprawnieniami udostępnienia.

© Acronis International GmbH, 2003-2024

Ważne
Folder **Udostępnione mi** nie jest uwzględniany w kopii zapasowej.

Ograniczenia

- Z powodu ograniczeń interfejsu API Dysku Google nie można utworzyć kopii zapasowej Dysku udostępnionego bez członków.
- Spośród formatów plików oprogramowania Google podczas operacji tworzenia kopii zapasowych w pełni są obsługiwane tylko dokumenty Google, arkusze Google i slajdy prezentacji Google. Inne formaty oprogramowania Google mogą nie być w pełni obsługiwane lub mogą wcale nie być obsługiwane. Na przykład pliki oprogramowania Rysunki Google są odzyskiwane jako pliki `.svg`, pliki oprogramowania Witryny Google — jako pliki `.txt`, pliki oprogramowania Google Jamboard — jako pliki `.pdf`, a pliki oprogramowania Moje Mapy Google są pomijane podczas tworzenia kopii zapasowej.

  Uwaga
  Formaty plików, które nie są specyficzne dla oprogramowania Google — takie jak `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png` czy `.zip` — są w pełni obsługiwane podczas tworzenia kopii zapasowej i odzyskiwania.

Jakie elementy można odzyskać?

Można odzyskać cały Dysk udostępniony lub dowolny plik bądź folder, który został uwzględniony w kopii zapasowej.

Można wybrać opcję odzyskania uprawnień udostępnienia lub dziedziczenia przez pliki uprawnień z folderu, do którego są odzyskiwane.

Następujące elementy nie są odzyskiwane:

- Jeśli w docelowym Dysku udostępnionym jest wyłączone udostępnianie plików osobom spoza danej organizacji, uprawnienia udostępnienia pliku, który został udostępniony użytkownikowi spoza organizacji, nie są odzyskiwane.
- Jeśli w docelowym Dysku udostępnionym jest wyłączona opcja **Udostępnianie osobom niebędącym członkami**, uprawnienia udostępnienia pliku, który został udostępniony użytkownikowi niebędącemu członkiem docelowego Dysku udostępnionego, nie są odzyskiwane.

Ograniczenia

- Komentarze zamieszczone w plikach nie są odzyskiwane.
- Nie można odzyskać łączy umożliwiających udostępnianie plików i folderów.

Wybieranie plików z Dysku udostępnionego

Wybierz pliki zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

© Acronis International GmbH, 2003-2024

Aby wybrać pliki z Dysku udostępnionego

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, w której przypadku chcesz utworzyć kopię zapasową danych użytkowników. W przeciwnym razie pomiń ten krok.
3. Wykonaj jedną z następujących czynności:
   - Aby utworzyć kopię zapasową plików ze wszystkich Dysków udostępnionych (w tym Dysków udostępnionych, które zostaną utworzone w przyszłości), rozwiń węzeł **Dyski udostępnione**, wybierz **Wszystkie Dyski udostępnione**, a następnie kliknij **Kopia zapasowa grupy**.
   - Aby utworzyć kopię zapasową plików z wybranych Dysków udostępnionych, rozwiń węzeł **Dyski udostępnione**, wybierz **Wszystkie Dyski udostępnione**, wskaż Dyski udostępnione, które chcesz uwzględnić w kopii zapasowej, a następnie kliknij **Kopia zapasowa**.
4. W panelu planu ochrony:
   - W obszarze **Elementy uwzględniane w kopii zapasowej** wykonaj jedną z następujących czynności:
     - Zachowaj ustawienie domyślne **[Wszystkie]** (wszystkie pliki).
     - Określ pliki i foldery do uwzględnienia w kopii zapasowej, dodając ich nazwy lub ścieżki. Można używać symboli wieloznacznych (*, ** i ?). Aby uzyskać więcej informacji na temat określania ścieżek i stosowania symboli wieloznacznych, zobacz „Filtry plików”.
     - Określ pliki i foldery do uwzględnienia w kopii zapasowej, przeglądając je. Łącze **Przeglądaj** jest dostępne tylko w przypadku tworzenia planu ochrony dla jednego Dysku udostępnionego.
   - [Opcjonalnie] W obszarze **Elementy uwzględniane w kopii zapasowej** kliknij **Pokaż wykluczenia**, aby określić pliki i foldery, które mają zostać pominięte w procesie tworzenia kopii zapasowej.
     Wykluczenia plików mają wyższy priorytet niż wybór plików, tj. w przypadku wskazania tego samego pliku w obu polach zostanie on pominięty podczas tworzenia kopii zapasowej.
   - Aby włączyć notaryzację wszystkich plików wybranych do uwzględnienia kopii zapasowej, włącz przełącznik **Notaryzacja**. Więcej informacji o notaryzacji można znaleźć w sekcji „Notaryzacja”.

Odzyskiwanie Dysku udostępnionego i plików z Dysku udostępnionego

Odzyskiwanie całego Dysku udostępnionego

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Dyski udostępnione**, wybierz **Wszystkie Dyski udostępnione**, wskaż Dysk udostępniony, który chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

© Acronis International GmbH, 2003-2024

Jeśli Dysk udostępniony został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

Dyski udostępnione można wyszukiwać na podstawie nazwy. Symbole wieloznaczne nie są obsługiwane.

4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Cały Dysk udostępniony**.
6. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, kliknij **Organizacja Google Workspace**, aby wyświetlić, zmienić lub określić organizację docelową.

   Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wybrać nową organizację docelową spośród dostępnych zarejestrowanych organizacji.
7. W polu **Odzyskaj na dysk** wyświetl, zmień lub określ docelowy Dysk udostępniony lub docelowego użytkownika. W przypadku określenia użytkownika dane zostaną odzyskane na Dysk Google tego użytkownika.

   Domyślnie jest wybrany oryginalny Dysk udostępniony. Jeśli Dysk udostępniony nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelowy Dysk udostępniony lub docelowego użytkownika.
8. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania plików.
9. Kliknij **Rozpocznij odzyskiwanie**.
10. Wybierz jedną z następujących opcji zastępowania:

Opcja	Opis
Zastąp istniejący plik, jeśli jest starszy	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie jak plik źródłowy, ale starszy od niego, plik źródłowy zostanie zapisany w lokalizacji docelowej, zastępując starszą wersję.
Zastąp istniejące pliki	Wszystkie pliki w lokalizacji docelowej zostaną zastąpione, niezależnie od daty ich ostatniej modyfikacji.
Nie zastępuj istniejących plików	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie, nie zostaną do niego zastosowane żadne zmiany, a plik źródłowy nie zostanie zapisany w lokalizacji docelowej.

11. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Odzyskiwanie plików z Dysku udostępnionego

1. Kliknij **Google Workspace**.
2. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, wybierz tę organizację, której dane chcesz odzyskać z kopii zapasowej. W przeciwnym razie pomiń ten krok.
3. Rozwiń węzeł **Dyski udostępnione**, wybierz **Wszystkie Dyski udostępnione**, wskaż Dysk udostępniony pierwotnie zawierający pliki, które chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.

© Acronis International GmbH, 2003-2024

Jeśli Dysk udostępniony został usunięty, wybierz go w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

Dyski udostępnione można wyszukiwać na podstawie nazwy. Symbole wieloznaczne nie są obsługiwane.

4. Wybierz punkt odzyskiwania.
5. Kliknij **Odzyskaj** > **Pliki/foldery**.
6. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych plików i folderów.
7. Wybierz pliki, które chcesz odzyskać.

   Jeśli kopia zapasowa nie jest zaszyfrowana i wybrano jeden plik, możesz kliknąć **Pokaż wersje**, aby wybrać wersję pliku do odzyskania. Możesz wybrać dowolną wersję uwzględnioną w kopii zapasowej przed wskazanym punktem odzyskiwania lub po nim.
8. Jeśli chcesz pobrać plik, zaznacz go, kliknij **Pobierz**, wybierz lokalizację, w której ma zostać zapisany plik, i kliknij **Zapisz**. W przeciwnym razie pomiń ten krok.
9. Kliknij **Odzyskaj**.
10. Jeśli do usługi Cyber Protection dodano wiele organizacji Google Workspace, kliknij **Organizacja Google Workspace**, aby wyświetlić, zmienić lub określić organizację docelową.

    Domyślnie wybrana jest pierwotna organizacja. Jeśli ta organizacja nie jest już zarejestrowana w usłudze Cyber Protection, trzeba wybrać nową organizację docelową spośród dostępnych zarejestrowanych organizacji.
11. W polu **Odzyskaj na dysk** wyświetl, zmień lub określ docelowy Dysk udostępniony lub docelowego użytkownika. W przypadku określenia użytkownika dane zostaną odzyskane na Dysk Google tego użytkownika.

    Domyślnie jest wybrany oryginalny Dysk udostępniony. Jeśli Dysk udostępniony nie istnieje lub wybrano organizację inną niż pierwotna, trzeba określić docelowy Dysk udostępniony lub docelowego użytkownika.
12. W polu **Ścieżka** wyświetl lub zmień folder docelowy w docelowym Dysku udostępnionym lub Dysku Google docelowego użytkownika. Domyślnie jest wybrana pierwotna lokalizacja.
13. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania plików.
14. Kliknij **Rozpocznij odzyskiwanie**.
15. Wybierz jedną z następujących opcji zastępowania plików:

Opcja	Opis
Zastąp istniejący plik, jeśli jest starszy	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie jak plik źródłowy, ale starszy od niego, plik źródłowy zostanie zapisany w lokalizacji docelowej, zastępując starszą wersję.
Zastąp istniejące pliki	Wszystkie pliki w lokalizacji docelowej zostaną zastąpione, niezależnie od daty ich ostatniej modyfikacji.
Nie zastępuj	Jeśli w lokalizacji docelowej znajduje się plik o takiej samej nazwie, nie zostaną do

© Acronis International GmbH, 2003-2024

Opcja	Opis
istniejących plików	niego zastosowane żadne zmiany, a plik źródłowy nie zostanie zapisany w lokalizacji docelowej.

16. Kliknij **Kontynuuj**, aby potwierdzić decyzję.

Notaryzacja

Notaryzacja pozwala udowodnić, że plik jest autentyczny i niezmieniony od momentu uwzględnienia w kopii zapasowej. Notaryzację warto włączyć w przypadku tworzenia kopii zapasowej plików dokumentów prawnych lub innych plików, które wymagają potwierdzenia autentyczności.

Notaryzacja jest dostępna tyko w przypadku kopii zapasowych plików z Dysku Google i Dysków udostępnionych Google Workspace.

Jak korzystać z funkcji notaryzacji

Aby włączyć notaryzację wszystkich plików wybranych do uwzględnienia w kopii zapasowej, włącz przełącznik **Notaryzacja** podczas tworzenia planu ochrony.

W ramach konfiguracji odzyskiwania notaryzowane pliki będą oznaczone specjalną ikoną i będzie można zweryfikować ich autentyczność.

Sposób działania

Podczas tworzenia kopii zapasowej agent oblicza kody skrótów uwzględnianych w kopii plików, buduje drzewo skrótów (na podstawie struktury folderów), zapisuje drzewo w kopii zapasowej, a następnie wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji zapisuje główne drzewo skrótów w bazie danych łańcucha bloków Ethereum, aby zapewnić, że ta wartość nie zostanie zmieniona.

Weryfikując autentyczność pliku, agent oblicza jego skrót, a następnie porównuje go ze skrótem przechowywanym w drzewie skrótów w kopii zapasowej. W przypadku niezgodności skrótów uznaje się, że plik nie jest autentyczny. W przeciwnym razie autentyczność plików jest gwarantowana przez drzewo skrótów.

Aby zweryfikować, czy samo drzewo skrótów nie zostało naruszone, agent wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji porównuje je z drzewem przechowywanym w bazie danych łańcucha bloków. Jeśli skróty są zgodne, wybrany plik otrzymuje gwarancję autentyczności. W przeciwnym razie program wyświetla komunikat, że plik nie jest autentyczny.

Weryfikowanie autentyczności pliku przy użyciu usługi Notary

Jeśli podczas tworzenia kopii zapasowej była włączona notaryzacja, istnieje możliwość weryfikacji autentyczności pliku uwzględnionego w kopii zapasowej.

Aby zweryfikować autentyczność pliku

© Acronis International GmbH, 2003-2024

1. Wykonaj jedną z następujących czynności:
   - Aby zweryfikować autentyczność pliku z Dysku Google, wybierz plik zgodnie z opisem podanym w krokach 1–7 w sekcji „Odzyskiwanie plików z Dysku Google”.
   - Aby zweryfikować autentyczność pliku z Dysku udostępnionego Google Workspace, wybierz plik zgodnie z opisem podanym w krokach 1–7 w sekcji „Odzyskiwanie plików z Dysku udostępnionego”.
2. Sprawdź, czy wybrany plik jest oznaczony następującą ikoną: . Oznacza to, że plik został notaryzowany.
3. Wykonaj jedną z następujących czynności:
   - Kliknij opcję **Sprawdź**.
     Program sprawdza autentyczność pliku i wyświetla wynik.
   - Kliknij opcję **Uzyskaj certyfikat**.
     Certyfikat potwierdzający notaryzację pliku zostanie otwarty w oknie przeglądarki internetowej. Okno to zawiera również instrukcje umożliwiające ręczną weryfikację autentyczności pliku.

Wyszukiwanie w kopiach zapasowych z chmury do chmury

W przypadku odzyskiwania danych możesz korzystać z funkcji wyszukiwania określonych elementów kopii zapasowej, zamiast przeglądać archiwum kopii zapasowych.

W przypadku niezaszyfrowanych kopii zapasowych wyszukiwanie jest zawsze dostępne. Obsługiwane jest tylko wyszukiwanie rozszerzone (oparte na indeksie).

Wyszukiwanie oparte na indeksie jest szybsze i oferuje dodatkowe opcje, takie jak pokazywanie wersji elementów uwzględnionych w kopii zapasowej, wyszukiwanie w nazwach załączników oraz wyszukiwanie pełnotekstowe w kopii zapasowej usługi Gmail.

Wyszukiwanie pełnotekstowe

Wyszukiwanie pełnotekstowe jest dostępne tylko w przypadku kopii zapasowych usługi Gmail i jest domyślnie włączone. Dzięki temu możesz przeszukiwać zawartość zarchiwizowanych wiadomości e-mail. Jeśli ta opcja jest wyłączona, możesz wyszukiwać tylko według tematu, nadawcy, odbiorcy i daty.

Pełnotekstowy indeks wyszukiwania zajmuje od 10 do 30 procent miejsca w pamięci masowej zajmowanego przez kopię zapasową usługi Gmail. Indeks bez danych wyszukiwania pełnotekstowego jest znacznie mniejszy. Aby zaoszczędzić miejsce w pamięci masowej, możesz wyłączyć wyszukiwanie pełnotekstowe i wyczyścić tę część indeksu, w której się znajdują dane wyszukiwania pełnotekstowego.

© Acronis International GmbH, 2003-2024

Indeksy wyszukiwania

Indeksy wyszukiwania zapewniają rozszerzone możliwości wyszukiwania w archiwum kopii zapasowych z chmury do chmury.

Archiwa są automatycznie indeksowane po każdej operacji tworzenia kopii zapasowej. Proces indeksowania nie wpływa na wydajność tworzenia kopii zapasowej, ponieważ indeksowanie i tworzenie kopii zapasowej są wykonywane przez różne komponenty oprogramowania.

Wyświetlenie wyników wyszukiwania jest możliwe po zakończeniu operacji indeksowania, która może trwać do 24 godzin. Indeksowanie pierwszej kopii zapasowej, która jest pełna, zwykle trwa dłużej niż indeksowanie kolejnych przyrostowych kopii zapasowych.

Wszystkie indeksy zawierają metadane, które obsługują główną funkcję wyszukiwania — wyszukiwanie według tematu, nadawcy, odbiorcy lub daty. Indeksy kopii zapasowych usługi Gmail zawierają dodatkowe dane, jeśli jest włączone wyszukiwanie pełnotekstowe.

Sprawdzanie rozmiaru indeksu wyszukiwania

Indeksy wyszukiwania z czasem stają się większe. Indeksy dla archiwum kopii zapasowej, w którym włączone jest wyszukiwanie pełnotekstowe, mogą zajmować nawet 30 procent rozmiaru archiwum.

Aby sprawdzić rozmiar indeksu wyszukiwania

1. Zaloguj się do konsoli Cyber Protect jako administrator.
2. Na karcie **Magazyn kopii zapasowych** kliknij **Kopia zapasowa aplikacji w chmurze**.
3. Sprawdź wartość w kolumnie **Rozmiar Indeksu**.

Aktualizowanie, odbudowywanie lub usuwanie indeksów

Aby rozwiązywać problemy związane z wyszukiwaniem w kopiach zapasowych z chmury do chmury, możesz aktualizować, odbudowywać lub usuwać indeksy wyszukiwania.

Uwaga
Przed aktualizacją, odbudową lub usunięciem indeksu warto skontaktować się z działem pomocy technicznej.

Aby zaktualizować, odbudować lub usunąć indeks

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Na karcie **Magazyn kopii zapasowych** kliknij **Kopia zapasowa aplikacji w chmurze**.
   Wybierz archiwum, którego indeks chcesz zaktualizować, przebudować lub usunąć.
   Dostępność tych czynności zależy od poziomu i roli administratora w sposób następujący:

© Acronis International GmbH, 2003-2024

Poziom konta	Rola	Może aktualizować indeks	Może utworzyć indeks ponownie	Może usunąć indeks
Dzierżawca-partner	Administrator firmy	+	+	+
	Administrator ochrony cybernetycznej	+	-	-
	Administrator ochrony	+	-	-
	Administrator ochrony w trybie tylko do odczytu	-	-	-
Dzierżawca-klient	Administrator firmy	+	-	-
	Administrator ochrony	+	-	-
	Administrator ochrony w trybie tylko do odczytu	-	-	-
Jednostka	Administrator jednostki	+	-	-
	Administrator ochrony	+	-	-
	Administrator ochrony w trybie tylko do odczytu	-	-	-

3. W panelu **Czynności** wybierz czynność, która ma zostać wykonana:
   - **Aktualizuj indeks** — zostaną sprawdzone punkty odzyskiwania w archiwum i dodane brakujące indeksy.
   - **Odbuduj indeks** — indeksy wszystkich punktów odzyskiwania w archiwum zostaną usunięte, a następnie utworzone ponownie.
   - **Usuń indeks** — zostaną usunięte indeksy wszystkich punktów odzyskiwania w archiwum.
4. [W przypadku archiwów zaszyfrowanych] Podaj hasło szyfrowania, a następnie kliknij **OK**.
5. Wybierz zakres czynności, a następnie kliknij **OK**.
   W zależności od archiwum i wybranej czynności dostępna jest jedna lub więcej z następujących opcji:
   - **Tylko metadane**
   - **Tylko zawartość**
   - **Przeszukiwanie metadanych i zawartości**

© Acronis International GmbH, 2003-2024

Wyłączanie wyszukiwania pełnotekstowego w przypadku kopii zapasowych usługi Gmail

Wyszukiwanie pełnotekstowe jest dostępne tylko w przypadku kopii zapasowych usługi Gmail i jest domyślnie włączone. Dzięki temu możesz przeszukiwać zawartość zarchiwizowanych wiadomości e-mail. Jeśli ta opcja jest wyłączona, możesz wyszukiwać tylko według tematu, nadawcy, odbiorcy i daty.

Jeśli musisz utrzymywać minimalny rozmiar indeksu wyszukiwania, możesz zechcieć wyłączyć wyszukiwanie pełnotekstowe.

Aby wyłączyć wyszukiwanie pełnotekstowe

1. Podczas tworzenia lub edycji planu tworzenia kopii zapasowych kliknij ikonę koła zębatego w prawym górnym rogu.
2. Na karcie **Wyszukiwanie pełnotekstowe** wyłącz przełącznik.
3. Kliknij **Gotowe**.
4. [W przypadku tworzenia planu] Kliknij **Zastosuj**.
5. [W przypadku edycji plan] Kliknij **Zapisz ustawienia**.

Uwaga
Jeśli ponownie włączysz wyszukiwanie pełnotekstowe, wszystkie archiwa utworzone przez ten plan tworzenia kopii zapasowych zostaną ponownie zindeksowane. Jest to czasochłonna operacja.

Ochrona systemu Oracle Database

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Metody ochrony systemu Oracle Database opisano w osobnym dokumencie dostępnym pod adresem https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf.

Ochrona platformy SAP HANA

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Metody ochrony platformy SAP HANA opisano w osobnym dokumencie dostępnym pod adresem: https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf

© Acronis International GmbH, 2003-2024

Chronienie danych z baz MySQL i MariaDB

Dane z baz MySQL i MariaDB można chronić przy użyciu kopii zapasowej uwzględniającej aplikacje. Przechowuje ona zebrane metadane aplikacji i umożliwia granularne odzyskiwanie na poziomie instancji, bazy danych lub tabeli.

Uwaga
Funkcja tworzenia kopii zapasowych uwzględniających aplikacje na potrzeby danych z bazy MySQL lub MariaDB jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Aby chronić za pomocą kopii zapasowych komputer fizyczny lub maszynę wirtualną, na których znajduje się instancja programu MySQL lub MariaDB, trzeba na nich zainstalować agenta dla MySQL/MariaDB. Agent dla MySQL/MariaDB jest dostępny w pakiecie z agentem dla systemu Linux (wersja 64-bitowa), w związku z czym może być instalowany tylko w 64-bitowych systemach operacyjnych Linux. Zobacz "Obsługiwane systemy operacyjne i środowiska" (s. 23).

Aby pobrać plik instalacyjny agenta dla systemu Linux (wersja 64-bitowa)

1. Zaloguj się do konsoli Cyber Protect.
2. Kliknij ikonę konta w prawym górnym rogu, a następnie wybierz **Do pobrania**.
3. Kliknij **Agent dla systemu Linux (wersja 64-bitowa)**.

   Plik instalacyjny zostanie pobrany na komputer. Aby zainstalować agenta, przejdź do czynności opisanych w sekcji "Instalowanie agentów ochrony w systemie Linux" (s. 87) lub "Instalowanie i odinstalowywanie agentów ochrony w systemie Linux" (s. 110). Koniecznie zaznacz opcję Agent dla MySQL/MariaDB, który jest komponentem opcjonalnym.

   Aby można było odzyskać bazy danych i tabele do działającej instancji, agent dla MySQL/MariaDB potrzebuje do działania tymczasowego magazynu. Domyślnie jest używany katalog `/tmp`. Możesz zmienić ten katalog przez ustawienie zmiennej środowiskowej `ACRONIS_MYSQL_RESTORE_DIR`.

Ograniczenia

- Klastry MySQL i MariaDB nie są obsługiwane.
- Instancje programów MySQL i MariaDB działające w kontenerach Docker nie są obsługiwane.
- Instancje programów MySQL i MariaDB działające w systemach operacyjnych korzystających z systemu plików BRTFS nie są obsługiwane.
- Systemowych baz danych (`sys`, `mysql`, `information-schema` i `performance_schema`) oraz baz danych, które nie zawierają żadnych tabel, nie można odzyskiwać do działających instancji. Bazy te można jednak odzyskiwać jako pliki podczas odzyskiwania całych instancji.
- Odzyskiwanie jest obsługiwane tylko w przypadku instancji docelowych w tej samej wersji co instancja uwzględniona w kopii zapasowej lub nowszej, ale występują następujące ograniczenia:
  - Odzyskiwanie z instancji programu MySQL 5.x do instancji programu MySQL 8.x nie jest obsługiwane.

© Acronis International GmbH, 2003-2024

- Odzyskiwanie do nowszej wersji programu MySQL 5.x (dotyczy to również wersji pomocniczych) jest obsługiwane tylko w ramach odzyskiwania całej instancji w postaci plików. Przed podjęciem próby odzyskania danych należy się zapoznać z oficjalnym podręcznikiem uaktualniania programu MySQL dotyczącym wersji docelowej, na przykład podręcznikiem uaktualniania dotyczącym programu MySQL 5.7.

- Odzyskiwanie z kopii zapasowych przechowywanych na partycji Secure Zone nie jest obsługiwane.
- Baz danych ani tabel nie można odzyskiwać za pomocą agenta dla MySQL/MariaDB działającego na komputerze, na którym jest zainstalowany moduł zabezpieczeń AppArmor. Wciąż jednak można odzyskać instancję jako pliki lub cały komputer.
- Odzyskiwanie do docelowych baz danych, które skonfigurowano przy użyciu łączy symbolicznych, nie jest obsługiwane. Możesz odzyskać bazy danych uwzględnione w kopii zapasowej jako nowe bazy, zmieniając ich nazwy.

Znane problemy

Jeśli podczas odzyskiwania danych z udziałów Samby chronionych hasłem napotkasz problemy, wyloguj się z konsoli Cyber Protect, a następnie zaloguj do niej ponownie. Wybierz odpowiedni punkt odzyskiwania, a następnie kliknij **Bazy danych MySQL/MariaDB**. Nie klikaj pozycji **Cały komputer** ani **Pliki/foldery**.

Konfigurowanie kopii zapasowej uwzględniającej aplikacje

Wymagania wstępne

- Na wybranym komputerze musi być uruchomiona co najmniej jedna instancja programu MySQL lub MariaDB.
- Na komputerze, na którym jest uruchomiona instancja programu MySQL lub MariaDB, trzeba uruchomić agenta ochrony na koncie użytkownika root.
- Kopia zapasowa uwzględniająca aplikacje jest dostępna tylko pod warunkiem, że w planie ochrony jako źródło kopii zapasowej wybrano opcję **Cały komputer**.
- Opcja tworzenia kopii zapasowej **Sektor po sektorze** w planie ochrony musi być wyłączona. W przeciwnym razie nie będzie można odzyskać danych aplikacji.

Aby skonfigurować kopię zapasową uwzględniającą aplikacje

1. W konsoli Cyber Protect wybierz co najmniej jeden komputer, na którym jest uruchomiona instancja programu MySQL lub MariaDB.
   Na każdym komputerze może być więcej niż jedna instancja.
2. Utwórz plan ochrony z włączonym modułem kopii zapasowej.
3. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Cały komputer**.
4. Kliknij **Kopia zapasowa aplikacji** i włącz przełącznik obok pozycji **MySQL/MariaDB Server**.
5. Wskaż, jak mają zostać określone instancje programu MySQL lub MariaDB:

© Acronis International GmbH, 2003-2024

- **W przypadku wszystkich obciążeń**

  Użyj tej opcji, jeśli uruchamiasz instancje o takiej samej konfiguracji na wielu serwerach. W przypadku każdej instancji będą używane te same parametry połączenia i poświadczenia dostępu.
- **W przypadku określonych obciążeń**

  Użyj tej opcji, aby określić parametry połączenia i poświadczenia dostępu dla każdej instancji.

6. Kliknij **Dodaj instancję**, aby skonfigurować parametry połączenia i poświadczenia dostępu.
   a. Wybierz typ połączenia, a następnie podaj następujące informacje:
      - [W przypadku gniazda TCP] Adres IP i port.
      - [W przypadku gniazda Unix] Ścieżka gniazda.
   b. Podaj poświadczenia konta użytkownika, które ma następujące uprawnienia do instancji:
      - `FLUSH_TABLES` lub `RELOAD` w przypadku wszystkich baz danych i tabel (`*.*`)
      - `SELECT` w przypadku `information_schema.tables`
   c. Kliknij **OK**.
7. Kliknij **Gotowe**.

Odzyskiwanie danych z kopii zapasowej uwzględniającej aplikacje

Z kopii zapasowej uwzględniającej aplikacje można odzyskiwać instancje programów MySQL i MariaDB, bazy danych oraz tabele. Można też odzyskać cały serwer, na którym działają instancje, albo pliki i foldery z tego serwera.

W poniższej tabeli zestawiono wszystkie opcje odzyskiwania.

Elementy do odzyskania	Obiekt docelowy odzyskiwania	Odzyskaj do
Serwer MySQL Serwer MariaDB	Cały komputer	Komputer*, na którym jest zainstalowany agent dla systemu Linux
Serwer MySQL Serwer MariaDB	Pliki lub foldery	Komputer*, na którym jest zainstalowany agent dla systemu Linux
Instancja	Pliki	Komputer*, na którym jest zainstalowany agent dla MySQL/MariaDB
Baza danych	Ta sama baza danych Nowa baza danych	Komputer*, na którym jest zainstalowany agent dla MySQL/MariaDB • Oryginalna instancja • Inna instancja

© Acronis International GmbH, 2003-2024

Elementy do odzyskania	Obiekt docelowy odzyskiwania	Odzyskaj do
		• Oryginalna baza danych • Nowa baza danych
Tabela	Ta sama tabela Nowa tabela	Komputer*, na którym jest zainstalowany agent dla MySQL/MariaDB • Oryginalna instancja • Inna instancja • Oryginalna baza danych • Pierwotna tabela • Nowa tabela

* Maszyna wirtualna zawierająca agenta jest z perspektywy tworzenia kopii zapasowych traktowana tak jak komputer fizyczny.

Odzyskiwanie całego serwera

Aby się dowiedzieć, jak odzyskać cały serwer, na którym jest uruchomiona instancja programu MySQL lub MariaDB, zobacz sekcję "Odzyskiwanie komputera" (s. 536).

Odzyskiwanie instancji

Z kopii zapasowej uwzględniającej aplikacje można odzyskiwać instancje programów MySQL i MariaDB w postaci plików.

Aby odzyskać instancję

1. W konsoli Cyber Protect wybierz komputer, który pierwotnie zawierał dane do odzyskania.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji. Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj jedną z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer z agentem dla MySQL/MariaDB i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie **Magazyn kopii zapasowych**.

   Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania.
4. Kliknij **Odzyskaj** > **Bazy danych MySQL/MariaDB**.
5. Wybierz instancję, którą chcesz odzyskać, a następnie kliknij **Odzyskaj jako pliki**.
6. W obszarze **Ścieżka** wybierz katalog, do którego mają zostać odzyskane pliki.
7. Kliknij **Rozpocznij odzyskiwanie**.

© Acronis International GmbH, 2003-2024

Odzyskiwanie baz danych

Z kopii zapasowej uwzględniającej aplikacje można odzyskiwać bazy danych do działających instancji programów MySQL i MariaDB.

1. W konsoli Cyber Protect wybierz komputer, który pierwotnie zawierał dane do odzyskania.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj jedną z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer z agentem dla MySQL/MariaDB i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie **Magazyn kopii zapasowych**.

   Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania.
4. Kliknij **Odzyskaj** > **Bazy danych MySQL/MariaDB**.
5. Kliknij nazwę odpowiedniej instancji, aby przejść do jej baz danych.
6. Wybierz co najmniej jedną bazę danych do odzyskania.
7. Kliknij **Odzyskaj**.
8. Kliknij **Docelowa instancja bazy danych MySQL/MariaDB**, aby określić parametry połączenia i poświadczenia dostępu dla instancji docelowej.
   - Sprawdź instancję, do której chcesz odzyskać dane. Domyślnie jest wybierana pierwotna instancja.
   - Podaj poświadczenia konta użytkownika, które ma uprawnienia dostępu do instancji docelowej. To konto użytkownika musi mieć przypisane następujące uprawnienia do wszystkich baz danych i tabel (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - Kliknij **OK**.
9. Zweryfikuj docelową bazę danych.

   Domyślnie jest wybrana pierwotna baza danych.

   Aby odzyskać bazę danych jako nową bazę, kliknij nazwę docelowej bazy danych i ją zmień. Działanie to jest dostępne tylko w przypadku odzyskiwania jednej bazy danych.

© Acronis International GmbH, 2003-2024

10. W obszarze **Zastąp istniejące bazy danych** wybierz tryb zastępowania.

    Domyślnie zastępowanie jest włączone, a baza danych uwzględniona w kopii zapasowej zastąpi docelową bazę o tej samej nazwie.

    Jeśli zastępowanie jest wyłączone, baza danych uwzględniona w kopii zapasowej zostanie pominięta podczas operacji odzyskiwania i nie zastąpi docelowej bazy o tej samej nazwie.
11. Kliknij **Rozpocznij odzyskiwanie**.

Odzyskiwanie tabel

Z kopii zapasowej uwzględniającej aplikacje można odzyskiwać tabele do działających instancji programów MySQL i MariaDB.

1. W konsoli Cyber Protect wybierz komputer, który pierwotnie zawierał dane do odzyskania.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj jedną z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer z agentem dla MySQL/MariaDB i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie **Magazyn kopii zapasowych**.

   Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania.
4. Kliknij **Odzyskaj** > **Bazy danych MySQL/MariaDB**.
5. Kliknij nazwę odpowiedniej instancji, aby przejść do jej baz danych.
6. Kliknij nazwę odpowiedniej bazy danych, aby przejść do jej tabel.
7. Wybierz co najmniej jedną tabelę, którą chcesz odzyskać.
8. Kliknij **Odzyskaj**.
9. Kliknij **Docelowa instancja bazy danych MySQL/MariaDB**, aby określić parametry połączenia i poświadczenia dostępu dla instancji docelowej.
   - Sprawdź instancję, do której chcesz odzyskać dane. Domyślnie jest wybierana pierwotna instancja.
   - Podaj poświadczenia konta użytkownika, które ma uprawnienia dostępu do instancji docelowej. To konto użytkownika musi mieć przypisane następujące uprawnienia do wszystkich baz danych i tabel (`*.*`):
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`

© Acronis International GmbH, 2003-2024

- ALTER
- SELECT

- Kliknij **OK**.

10. Zweryfikuj tabelę docelową.
    Domyślnie jest wybrana pierwotna tabela.
    Aby odzyskać tabelę jako nową, kliknij nazwę tabeli docelowej i ją zmień. Działanie to jest dostępne tylko w przypadku odzyskiwania jednej tabeli.
11. W obszarze **Zastąp istniejące tabele** wybierz tryb zastępowania.
    Domyślnie zastępowanie jest włączone, a tabela uwzględniona w kopii zapasowej zastąpi docelową tabelę o tej samej nazwie.
    Jeśli zastępowanie jest wyłączone, tabela uwzględniona w kopii zapasowej zostanie pominięta podczas operacji odzyskiwania i nie zastąpi docelowej tabeli o tej samej nazwie.
12. Kliknij **Rozpocznij odzyskiwanie**.

Odzyskiwanie procedur składowanych

W przypadku odzyskiwania całej instancji MySQL procedury składowane są odzyskiwane automatycznie.

W przypadku odzyskiwania jednej bazy danych do innej instancji niż pierwotna lub odzyskiwania jej jako nowej bazy danych, procedury składowane nie są odzyskiwane automatycznie. Można je odzyskać ręcznie, eksportując je do pliku SQL, a następnie dodając do odzyskanej bazy danych.

Aby wyeksportować procedury składowane i je dodać do odzyskanej bazy danych

1. Na komputerze z pierwotną instancją MySQL otwórz narzędzie Terminal.
2. Uruchom następujące polecenie, aby wyeksportować procedury składowane.
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data > [exported_db_routines.sql]
   ```
4. Na komputerze, na który jest odzyskiwana baza danych, otwórz klienta wiersza polecenia MySQL.
5. Uruchom następujące polecenia, aby dodać procedury do odzyskanej bazy danych.

   ```
   mysql>  use [recovered_database_name];
   ```

   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```


© Acronis International GmbH, 2003-2024
   ```

Ochrona witryn internetowych i serwerów hostingu

Ochrona witryn internetowych

Wskutek nieautoryzowanego dostępu lub złośliwego ataku witryna internetowa może zostać uszkodzona. Jeśli chcesz mieć możliwość łatwego przywrócenia dobrego stanu uszkodzonej witryny internetowej, twórz jej kopie zapasowe.

Co jest potrzebne do utworzenia kopii zapasowej witryny internetowej?

Witryna internetowa musi być dostępna przy użyciu protokołu SFTP lub SSH. Nie trzeba instalować agenta. Wystarczy dodać witrynę internetową zgodnie z opisem zamieszczonym w dalszej części tej sekcji.

Jakie elementy można uwzględnić w kopii zapasowej?

W kopii zapasowej można uwzględnić następujące elementy:

- **Pliki zawartości witryny internetowej**
  Wszystkie pliki dostępne dla konta określonego na potrzeby połączenia SFTP lub SSH.
- **Połączone bazy danych (jeśli są dostępne) hostowane na serwerach MySQL.**
  Wszystkie bazy danych dostępne dla określonego konta MySQL.

Jeśli w witrynie internetowej są wykorzystywane bazy danych, najlepiej jest zrobić kopię zapasową zarówno plików, jak i baz danych, aby móc je odzyskać w stanie spójnym.

Ograniczenia

- Jedyną lokalizacją kopii zapasowych dostępną w przypadku witryn internetowych jest chmura.
- Do witryny internetowej można zastosować kilka planów ochrony, ale tylko jeden z nich może być uruchamiany według harmonogramu. Pozostałe plany trzeba uruchamiać ręcznie.
- Jedyną dostępną opcją dotyczącą kopii zapasowych jest „Nazwa pliku kopii zapasowej”.
- Plany ochrony witryn internetowych nie są widoczne na karcie **Zarządzanie** > **Plany ochrony**.

Tworzenie kopii zapasowej witryny internetowej

Aby dodać witrynę internetową

1. Kliknij **Urządzenia** > **Dodaj**.
2. Kliknij **Witryna internetowa**.
3. Skonfiguruj następujące ustawienia dostępu dla witryny internetowej:
   - W polu **Nazwa witryny internetowej** utwórz i wpisz nazwę witryny internetowej. Nazwa ta będzie wyświetlana w konsoli Cyber Protect.

© Acronis International GmbH, 2003-2024

- W polu **Host** określ nazwę lub adres IP hosta, które będą używane w celu uzyskania dostępu do witryny internetowej przy użyciu protokołu SFTP lub SSH. Na przykład `moj.serwer.com` lub `10.250.100.100`.
- W polu **Port** określ numer portu.
- W polach **Nazwa użytkownika** i **Hasło** określ poświadczenia konta, którego można używać w celu uzyskania dostępu do witryny internetowej przy użyciu protokołu SFTP lub SSH.

  Ważne
  W kopii zapasowej zostaną uwzględnione tylko pliki dostępne dla określonego tu konta.

  Zamiast hasła możesz określić klucz prywatny SSH. W tym celu zaznacz pole wyboru **Używaj klucza prywatnego SSH, a nie hasła** i określ klucz.

4. Kliknij **Dalej**.
5. Jeśli w witrynie internetowej są wykorzystywane bazy danych MySQL, skonfiguruj ustawienia dostępu do tych baz danych. W przeciwnym razie kliknij **Pomiń**.
   a. W polu **Typ połączenia** zaznacz sposób dostępu do baz danych z chmury:
      - **Za pośrednictwem protokołu SSH z hosta** — dostęp do baz danych będzie uzyskiwany z hosta określonego w kroku 3.
      - **Połączenie bezpośrednie** — dostęp do baz danych będzie uzyskiwany bezpośrednio. To ustawienie wybierz tylko wtedy, gdy bazy danych są dostępne z Internetu.

   b. W polu **Host** określ nazwę lub adres IP hosta, na którym działa MySQL Server.
   c. W polu **Port** określ numer portu na potrzeby połączenia TCP/IP z serwerem. Domyślnym numerem portu jest 3306.
   d. W polach **Nazwa użytkownika** i **Hasło** określ poświadczenia konta MySQL.

      Ważne
      W kopii zapasowej zostaną uwzględnione tylko bazy danych dostępne dla określonego tu konta.

   e. Kliknij **Utwórz**.

   Witryna internetowa pojawi się w konsoli Cyber Protect w obszarze **Urządzenia** > **Witryny internetowe**.

Aby zmienić ustawienia połączenia

1. Zaznacz witrynę internetową w obszarze **Urządzenia** > **Witryny internetowe**.
2. Kliknij opcję **Szczegóły**.
3. Kliknij ikonę ołówka obok witryny internetowej lub ustawień połączenia z bazą danych.
4. Wprowadź niezbędne zmiany i kliknij **Zapisz**.

Aby utworzyć plan ochrony dotyczący witryn internetowych

© Acronis International GmbH, 2003-2024

1. Zaznacz co najmniej jedną witrynę internetową w obszarze **Urządzenia** > **Witryny internetowe**.
2. Kliknij **Chroń**.
3. [Opcjonalnie] Włącz tworzenie kopii zapasowych baz danych.
   Jeśli wybrano kilka witryn internetowych, tworzenie kopii zapasowych baz danych jest domyślnie wyłączone.
4. [Opcjonalnie] Zmień reguły przechowywania.
5. [Opcjonalnie] Włącz szyfrowanie kopii zapasowych.
6. [Opcjonalnie] Kliknij ikonę koła zębatego, aby edytować opcję **Nazwa pliku kopii zapasowej**.
   Jest to dobre rozwiązanie w dwóch sytuacjach:
   - Została już utworzona kopia zapasowa witryny internetowej i chcesz kontynuować istniejącą sekwencję kopii
   - Chcesz, aby na karcie **Magazyn kopii zapasowych** była wyświetlana niestandardowa nazwa
7. Kliknij **Zastosuj**.

Plany ochrony dotyczące witryn internetowych można edytować, odwoływać i usuwać tak samo jak plany dotyczące komputerów. Operacje te opisano w sekcji „Operacje dotyczące planów ochrony”.

Odzyskiwanie witryny internetowej

Aby odzyskać witrynę internetową

1. Wykonaj jedną z następujących czynności:
   - W obszarze **Urządzenia** > **Witryny internetowe** zaznacz witrynę internetową, którą chcesz odzyskać, a następnie kliknij **Odzyskiwanie**.
     Witryny internetowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.
   - Jeśli witryna internetowa została usunięta, wybierz ją w sekcji **Kopie zapasowe aplikacji w chmurze** na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
     Aby odzyskać usuniętą witrynę internetową, trzeba dodać witrynę docelową jako urządzenie.
2. Wybierz punkt odzyskiwania.
3. Kliknij **Odzyskaj** i wybierz elementy do odzyskania: **Cała witryna internetowa**, **Bazy danych** (jeśli jakaś istnieje) lub **Pliki/foldery**.
   Aby się upewnić, że witryna internetowa jest w stanie spójnym, najlepiej jest przeprowadzić odzyskiwanie zarówno plików, jak i baz danych — w dowolnej kolejności.
4. W zależności od dokonanego wyboru wykonaj jedną z opisanych niżej procedur.

Aby odzyskać całą witrynę internetową

1. W obszarze **Odzyskaj do witryny internetowej** wyświetl lub zmień docelową witrynę internetową.
   Domyślnie wybrana jest oryginalna witryna internetowa. Jeśli ta witryna nie istnieje, trzeba wybrać docelową witrynę internetową.

© Acronis International GmbH, 2003-2024

2. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania odzyskiwanych plików.
3. Kliknij **Rozpocznij odzyskiwanie** i potwierdź czynność.

Aby odzyskać bazy danych

1. Wybierz bazy danych, które chcesz odzyskać.
2. Jeśli chcesz pobrać bazę danych jako plik, kliknij **Pobierz**, wybierz lokalizację, w której ma zostać zapisany plik, i kliknij **Zapisz**. W przeciwnym razie pomiń ten krok.
3. Kliknij **Odzyskaj**.
4. W obszarze **Odzyskaj do witryny internetowej** wyświetl lub zmień docelową witrynę internetową.
   Domyślnie wybrana jest oryginalna witryna internetowa. Jeśli ta witryna nie istnieje, trzeba wybrać docelową witrynę internetową.
5. Kliknij **Rozpocznij odzyskiwanie** i potwierdź czynność.

Aby odzyskać pliki/foldery witryny internetowej

1. Wybierz pliki/foldery, które chcesz odzyskać.
2. Jeśli chcesz zapisać plik, kliknij **Pobierz**, wybierz lokalizację, w której ma zostać zapisany plik, i kliknij **Zapisz**. W przeciwnym razie pomiń ten krok.
3. Kliknij **Odzyskaj**.
4. W obszarze **Odzyskaj do witryny internetowej** wyświetl lub zmień docelową witrynę internetową.
   Domyślnie wybrana jest oryginalna witryna internetowa. Jeśli ta witryna nie istnieje, trzeba wybrać docelową witrynę internetową.
5. Zdecyduj, czy chcesz odzyskać uprawnienia do udostępniania odzyskiwanych plików.
6. Kliknij **Rozpocznij odzyskiwanie** i potwierdź czynność.

Ochrona serwerów hostingu witryn internetowych

Istnieje możliwość chronienia serwerów hostingu witryn internetowych z systemem Linux oraz uruchomionym panelem sterowania Plesk, cPanel, DirectAdmin, VirtualMin lub ISPManager. Serwery, na których działają panele sterowania hostingu witryn internetowych innych producentów, są chronione jak zwykłe obciążenia.

Limity

Serwery z uruchomionym panelem sterowania Plesk, cPanel, DirectAdmin, VirtualMin lub ISPManager są uznawane za serwery hostingu witryn internetowych. Każdy serwer hostingu witryn internetowych uwzględniany w kopii zapasowej jest wliczany do przypisanego limitu **Serwery hostingu witryn internetowych**. W przypadku wyłączenia tego limitu lub przekroczenia jego nadwyżki zostanie przypisany limit zgodnie z poniższym opisem lub operacja tworzenia kopii zapasowej się nie powiedzie:

© Acronis International GmbH, 2003-2024

- W przypadku serwera fizycznego jest obciążany limit **Serwery**. W przypadku wyłączenia tego limitu lub przekroczenia jego nadwyżki operacja tworzenia kopii zapasowej się nie powiedzie.
- W przypadku serwera wirtualnego jest obciążany limit **Maszyny wirtualne**. W przypadku wyłączenia tego limitu lub przekroczenia jego nadwyżki operacja tworzenia kopii zapasowej się nie powiedzie.

Integracje z rozwiązaniami DirectAdmin, cPanel i Plesk

Administratorzy hostingu, którzy korzystają z rozwiązań DirectAdmin, Plesk lub cPanel, mogą integrować te panele sterowania z usługą Cyber Protection, aby móc korzystać z kilku wygodnych funkcji, w tym:

- Tworzenie w chmurze kopii zapasowych na poziomie dysku obejmujących cały serwer hostingowy
- Odzyskiwanie całego serwera, w tym wszystkich witryn internetowych i kont
- Odzyskiwanie granularne i pobieranie kont, witryn internetowych, wybranych plików, skrzynek pocztowych lub baz danych
- Umożliwianie sprzedawcom i klientom wykonywanie samodzielnego odzyskiwania własnych danych

W celu przeprowadzenia integracji należy użyć rozszerzenia usługi Cyber Protection. Aby uzyskać szczegółowe informacje, zapoznaj się z odpowiednimi przewodnikami integracji:

- Przewodnik integracji DirectAdmin
- Przewodnik integracji WHM i cPanel
- Przewodnik integracji Plesk

Specjalne operacje dotyczące maszyn wirtualnych

Uruchamianie maszyny wirtualnej z kopii zapasowej (Instant Restore)

Maszynę wirtualną można uruchomić z kopii zapasowej na poziomie dysku, która zawiera system operacyjny. Operacja ta, nazywana również przywracaniem błyskawicznym, umożliwia przygotowanie serwera wirtualnego w kilka sekund. Dyski wirtualne są emulowane bezpośrednio z kopii zapasowej, dzięki czemu nie zajmują miejsca w magazynie danych (magazynie). Miejsce w pamięci masowej jest wymagane wyłącznie w celu przechowywania zmian zachodzących na dyskach wirtualnych.

Taka tymczasowa maszyna wirtualna powinna działać do trzech dni. Po tym czasie można ją całkowicie usunąć lub przekształcić w zwykłą maszynę wirtualną (sfinalizować) bez przerywania jej działania.

Dopóki istnieje tymczasowa maszyna wirtualna, do używanej przez nią kopii zapasowej nie można stosować reguł przechowywania. Operacje tworzenia kopii zapasowych pierwotnej maszyny mogą być nadal uruchamiane.

© Acronis International GmbH, 2003-2024

Przykłady użycia

- **Odzyskiwanie po awarii**

  Można niezwłocznie udostępnić kopię uszkodzonej maszyny wirtualnej w trybie online.
- **Testowanie kopii zapasowych**

  Można uruchomić maszynę z kopii zapasowej i upewnić się, czy system operacyjny-gość i aplikacje działają prawidłowo.
- **Uzyskiwanie dostępu do danych aplikacji**

  W czasie działania maszyny można ocenić i wyodrębnić wymagane dane przy użyciu macierzystych narzędzi do zarządzania aplikacji.

Wymagania wstępne

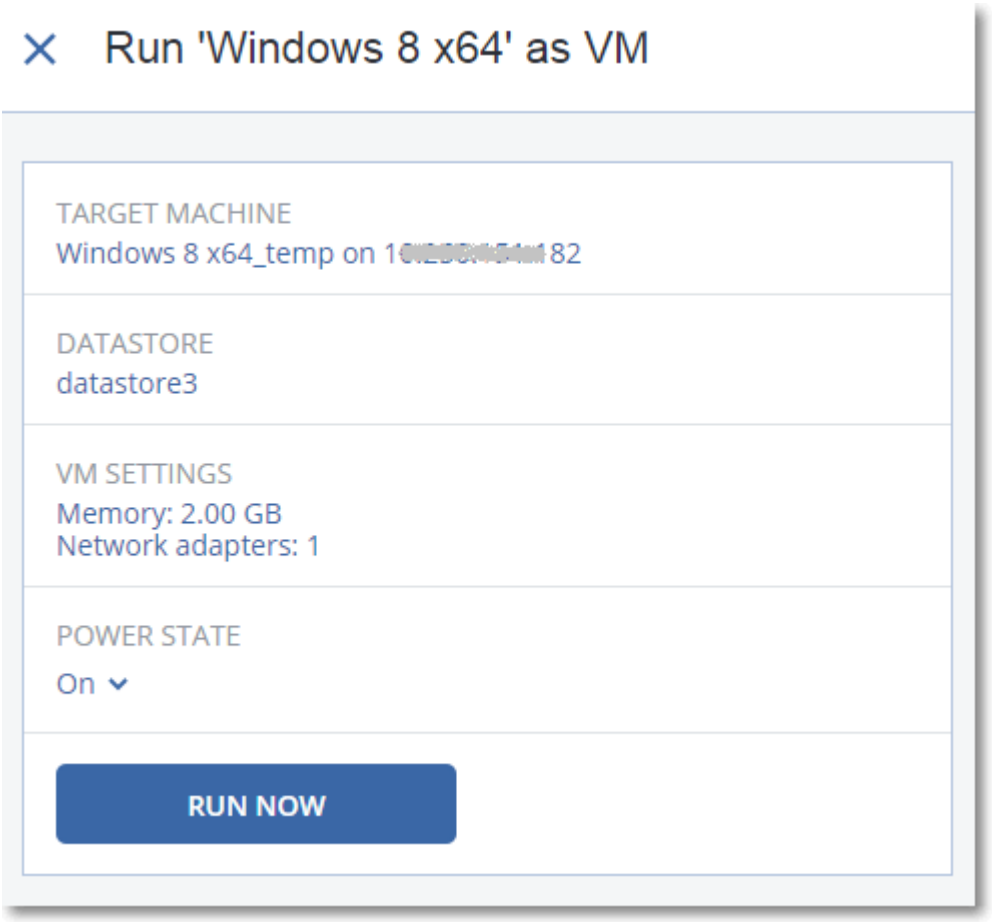
- W usłudze Cyber Protection musi być zarejestrowany co najmniej jeden agent dla VMware lub agent dla Hyper-V.
- Kopia zapasowa może być przechowywana w folderze sieciowym lub folderze lokalnym komputera z zainstalowanym agentem dla VMware lub agentem dla Hyper-V. Jeśli wybierzesz folder sieciowy, musi on być dostępny z danego komputera. Maszynę wirtualną można też uruchomić z kopii zapasowej przechowywanej w chmurze, ale wtedy będzie ona działać wolniej, ponieważ operacja ta wymaga intensywnych operacji odczytu losowego z kopii zapasowej.
- Kopia zapasowa musi zawierać cały komputer lub wszystkie woluminy wymagane do uruchomienia systemu operacyjnego.
- Można korzystać z kopii zapasowych zarówno komputerów fizycznych, jak i maszyn wirtualnych. Nie można korzystać z kopii zapasowych *kontenerów* Virtuozzo.
- Kopie zapasowe zawierające woluminy logiczne systemu Linux (LVM) muszą zostać utworzone przez agenta dla VMware lub agenta dla Hyper-V. Maszyna wirtualna musi być tego samego typu co pierwotna maszyna (ESXi lub Hyper-V).

Uruchamianie maszyny

1. Wykonaj jedną z następujących czynności:
   - Wybierz komputer uwzględniony w kopii zapasowej, kliknij **Odzyskaj**, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.
2. Kliknij **Uruchom jako maszynę wirtualną**.

   Program automatycznie wybierze host i inne wymagane parametry.

© Acronis International GmbH, 2003-2024



3. [Opcjonalnie] Kliknij **Komputer docelowy**, a następnie zmień typ maszyny wirtualnej (ESXi lub Hyper-V), host lub nazwę maszyny wirtualnej.
4. [Opcjonalnie] Kliknij **Magazyn danych** w przypadku maszyny ESXi lub **Ścieżka** w przypadku maszyny Hyper-V, a następnie wybierz magazyn danych dla maszyny wirtualnej.

   W czasie działania maszyny są gromadzone zmiany zachodzące na dyskach wirtualnych. Upewnij się, że w wybranym magazynie danych jest wystarczająco dużo wolnego miejsca. Jeśli zamierzasz zachować te zmiany przez skonfigurowanie maszyny wirtualnej jako trwałej, wybierz magazyn danych nadający się do obsługi tej maszyny w środowisku produkcyjnym.
5. [Opcjonalnie] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci oraz połączenia sieciowe maszyny wirtualnej.
6. [Opcjonalnie] Wybierz stan zasilania maszyny (**Włączono**/**Wyłączono**).
7. Kliknij **Uruchom teraz**.

W wyniku tego maszyna będzie pokazywana w interfejsie internetowym z jedną z następujących ikon: lub

. Takich maszyn wirtualnych nie można wybierać do uwzględnienia w kopii zapasowej.

© Acronis International GmbH, 2003-2024

Uwaga
Operację Uruchom jako maszynę wirtualną (błyskawiczne przywracanie) można wykonać w odniesieniu do kopii zapasowych na platformie Microsoft Azure. Operacja ta powoduje jednak znaczny ruch wychodzący, który zostanie uwzględniony na rachunku za subskrypcję platformy Microsoft Azure. Typowy ruch wychodzący w przypadku maszyny z systemem Windows uruchomionej z kopii zapasowej na platformie Microsoft Azure wynosiłby około 5 GB od włączenia maszyny wirtualnej do zalogowania się.

Usuwanie maszyny

Odradzamy usuwanie tymczasowych maszyn wirtualnych bezpośrednio w środowisku vSphere czy Hyper-V. Może to prowadzić do powstawania artefaktów w interfejsie internetowym. Ponadto, kopia zapasowa, z której została uruchomiona maszyna, może pozostać przez jakiś czas zablokowana (nie może zostać usunięta zgodnie z regułami przechowywania).

Aby usunąć maszynę wirtualną uruchomioną z kopii zapasowej

1. Na karcie **Wszystkie urządzenia** zaznacz maszynę uruchomioną z kopii zapasowej.
2. Kliknij **Usuń**.

Maszyna zostanie usunięta z interfejsu internetowego. Zostanie także usunięta z inwentaryzacji oraz magazynu danych (magazynu) vSphere lub Hyper-V. Wszelkie zmiany w danych wprowadzone w czasie działania maszyny zostaną utracone.

Finalizowanie maszyny

W przypadku uruchomienia maszyny wirtualnej z kopii zapasowej zawartość dysków wirtualnych jest pobierana bezpośrednio z tej kopii. Dlatego w przypadku utraty połączenia z lokalizacją kopii zapasowej lub agentem ochrony maszyna może przestać być dostępna lub nawet zostać uszkodzona.

Jest dostępna opcja przekształcenia maszyny w maszynę trwałą, tj. odzyskania wszystkich jej dysków wirtualnych, a także zmian, które zaszły w czasie działania maszyny, do magazynu danych przechowującego te zmiany. Proces ten określa się mianem finalizacji.

Finalizacja jest wykonywana bez przerywania działania. Maszyna wirtualna *nie* zostanie wyłączona w trakcie finalizacji.

Lokalizacja finalnych dysków wirtualnych jest określona w parametrach operacji **Uruchom jako maszynę wirtualną** (**Magazyn danych** w przypadku ESXi lub **Ścieżka** w przypadku Hyper-V). Przed rozpoczęciem finalizacji należy się upewnić, że wolne miejsce, możliwości udostępniania i wydajność magazynu danych są wystarczające, aby uruchomić maszynę w środowisku produkcyjnym.

© Acronis International GmbH, 2003-2024

Uwaga
Finalizacja nie jest obsługiwana w przypadku funkcji Hyper-V działającego w systemach Windows Server 2008/2008 R2 i Microsoft Hyper-V Server 2008/2008 R2, ponieważ w tych wersjach funkcji Hyper-V brakuje niezbędnego interfejsu API.

Aby sfinalizować maszynę uruchomioną z kopii zapasowej

1. Na karcie **Wszystkie urządzenia** zaznacz maszynę uruchomioną z kopii zapasowej.
2. Kliknij **Finalizuj**.
3. [Opcjonalnie] Określ nową nazwę maszyny.
4. [Opcjonalnie] Zmień tryb alokowania dysku. Ustawienie domyślne to **Elastyczne**.
5. Kliknij **Finalizuj**.

Nazwa maszyny zostanie natychmiast zmieniona. Na karcie **Działania** jest wyświetlany postęp odzyskiwania. Po ukończeniu odzyskiwania ikona maszyny zostanie zastąpiona ikoną zwykłej maszyny wirtualnej.

Co trzeba wiedzieć o finalizacji

Finalizacja a zwykłe odzyskiwanie

Proces finalizacji zajmuje więcej czasu niż zwykłe odzyskiwanie z następujących powodów:

- Podczas finalizacji agent losowo uzyskuje dostęp do różnych części kopii zapasowej. W przypadku odzyskiwania całej maszyny agent sekwencyjnie odczytuje dane z kopii zapasowej.
- Jeśli maszyna wirtualna działa podczas finalizacji, agent częściej odczytuje dane z kopii zapasowej, aby podtrzymać jednoczesne działanie obu procesów. Podczas zwykłego odzyskiwania maszyna wirtualna zostaje zatrzymana.

Finalizacja maszyn uruchomionych z kopii zapasowych w chmurze

Ze względu na intensywność uzyskiwania dostępu do danych kopii zapasowych szybkość finalizacji w dużym stopniu zależy od przepustowości łącza między lokalizacją kopii zapasowych a agentem. W przypadku kopii zapasowych znajdujących się w chmurze finalizacja zajmie więcej czasu niż w przypadku lokalnych kopii zapasowych. Jeśli połączenie z Internetem jest bardzo wolne lub niestabilne, finalizacja maszyny uruchomionej z kopii zapasowej w chmurze może się nie udać. Jeśli planujesz finalizację i masz wybór, najlepiej uruchom maszyny wirtualne z lokalnych kopii zapasowych.

© Acronis International GmbH, 2003-2024

Uwaga
Szybkość finalizacji zależy od tego, czy agent ma połączenie z hostem VMware ESXi, czy z serwerem vCenter, jak opisano w kroku 3 z "Konfigurowanie urządzenia wirtualnego" (s. 147). Połączenie z serwerem VMware vCenter może spowolnić operację finalizacji ze względu na specyfikę interfejsów API VMware. Aby przyspieszyć operację finalizacji, należy użyć osobnego agenta dla VMware w celu wykonania operacji **Uruchom jako maszynę wirtualną**, a po niej dokonać finalizacji, w ramach której agent będzie mieć połączenie z hostem ESXi, a nie serwerem vCenter.

Praca w środowisku VMware vSphere

W tej sekcji opisano operacje specyficzne dla środowisk VMware vSphere.

Replikacja maszyn wirtualnych

Replikacja jest dostępna tylko w przypadku maszyn wirtualnych VMware ESXi.

Proces replikacji polega na utworzeniu dokładnej kopii (repliki) maszyny wirtualnej, a następnie ciągłym synchronizowaniu repliki z pierwotną maszyną. Dzięki replikowaniu krytycznej maszyny wirtualnej zawsze będziesz dysponować gotową do uruchomienia kopią tej maszyny.

Replikację można rozpocząć ręcznie lub zgodnie z samodzielnie określonym harmonogramem. Pierwsza replikacja jest pełna (polega na utworzeniu kopii całej maszyny). Kolejne replikacje są przyrostowe. Wykonuje się je przy użyciu funkcji Changed Block Tracking, chyba że ta opcja jest wyłączona.

Replikacja a tworzenie kopii zapasowej

W odróżnieniu od zaplanowanych kopii zapasowych replika przechowuje tylko ostatni stan maszyny wirtualnej. Replika zajmuje miejsce w magazynie danych, podczas gdy kopii zapasowe można przechowywać w tańszym magazynie.

Z drugiej strony włączenie repliki trwa znacznie krócej niż operacja odzyskiwania i krócej niż uruchomienie maszyny wirtualnej z kopii zapasowej. Włączona replika działa znacznie szybciej niż maszyna wirtualna uruchomiona z kopii zapasowej i nie wymaga załadowania agenta dla VMware.

Przykłady użycia

- **Replikacja maszyny wirtualnej do lokalizacji zdalnej.**
  Replikacja pozwala na normalne funkcjonowanie w warunkach częściowej lub całkowitej awarii centrum danych dzięki sklonowaniu maszyn wirtualnych z lokalizacji podstawowej do dodatkowej. Lokalizacja dodatkowa zwykle znajduje się w innym obiekcie, któremu raczej nie zagraża problem środowiskowy czy infrastrukturowy ani żadne inne czynniki będące przyczyną ewentualnej awarii w lokalizacji podstawowej.
- **Replikacja maszyn wirtualnych w ramach jednej lokalizacji (z jednego hosta / magazynu danych do drugiego).**
  Replikację lokalną można stosować na potrzeby wysokiej dostępności lub odzyskiwania po awarii.

© Acronis International GmbH, 2003-2024

Możliwe zadania związane z repliką

- **Testowanie repliki**

  W celu przeprowadzenia testów replika zostanie włączona. Wówczas za pomocą klienta vSphere lub innych narzędzi należy sprawdzić, czy replika działa prawidłowo. Na czas testów replikacja zostanie zawieszona.
- **Przełączenie awaryjne na replikę**

  Przełączenie awaryjne polega na przeniesieniu obciążenia z pierwotnej maszyny wirtualnej na jej replikę. Na czas przełączenia awaryjnego replikacja zostanie zawieszona.
- **Tworzenie kopii zapasowej repliki**

  Operacje tworzenia kopii zapasowych i replikacji wymagają dostępu do dysków wirtualnych, w związku z czym obniżają wydajność hosta, na którym działa maszyna wirtualna. Jeśli chcesz mieć zarówno replikę, jak i kopie zapasowe maszyny wirtualnej, ale nie chcesz dodatkowo obciążać hosta produkcyjnego, zreplikuj maszynę na inny host i skonfiguruj tworzenie kopii zapasowych repliki.

Ograniczenia

- Nie można replikować maszyn wirtualnych następujących typów:
  - Maszyny odporne na awarie w środowisku ESXi w wersji 5.5 lub starszej
  - Maszyny uruchomione z kopii zapasowych
  - Repliki maszyn wirtualnych
- Niektóre zmiany sprzętowe, takie jak dodanie karty sieciowej do hosta ESXi lub usunięcie jej z niego, powodują zmianę wewnętrznych identyfikatorów hosta. Zmiana ta wpływa na plany replikacji maszyn wirtualnych. Po takiej zmianie należy ponownie utworzyć plany replikacji maszyn wirtualnych, w których jako lokalizację źródłową lub docelową był wybrany host ESXi – w przeciwnym razie wykonywanie tych planów będzie się kończyć niepowodzeniem.

Tworzenie planu replikacji

Plan replikacji trzeba utworzyć dla każdego komputera z osobna. Nie można zastosować istniejącego już planu do innych komputerów.

Aby utworzyć plan replikacji

1. Wybierz maszynę wirtualną do replikacji.
2. Kliknij **Replikacja**.

   W oprogramowaniu zostanie wyświetlony nowy szablon planu replikacji.
3. [Opcjonalnie] Aby zmodyfikować nazwę planu replikacji, kliknij nazwę domyślną.
4. Kliknij **Komputer docelowy**, a następnie zrób tak:
   a. Wybierz, czy ma zostać utworzona nowa replika, czy chcesz użyć istniejącej już repliki pierwotnego komputera.
   b. Wybierz host ESXi i określ nazwę nowej repliki lub wybierz replikę już istniejącą.

© Acronis International GmbH, 2003-2024

Domyślnie nowa replika ma nazwę **[Nazwa oryginalnego komputera]_replica**.

c. Kliknij **OK**.

5. [Tylko w przypadku replikacji na nową maszynę] Kliknij **Magazyn danych** i wybierz magazyn danych dla maszyny wirtualnej.
6. [Opcjonalnie] Kliknij **Harmonogram**, aby zmienić harmonogram replikacji.

   Domyślnie replikacje są wykonywane codziennie od poniedziałku do piątku. Można wybrać godzinę rozpoczęcia replikacji.

   Aby zmienić częstość replikacji, przesuń suwak i określ harmonogram.

   Możesz też:

   - Określić zakres dat wyznaczający okres obowiązywania harmonogramu. Zaznacz pole wyboru **Uruchom plan w danym przedziale dat**, a następnie określ zakres dat.
   - Wyłączyć harmonogram. W tym przypadku replikację można rozpocząć ręcznie.
7. [Opcjonalnie] Kliknij ikonę koła zębatego, aby zmodyfikować opcje replikacji.
8. Kliknij **Zastosuj**.
9. [Opcjonalnie] Aby uruchomić plan ręcznie, kliknij **Uruchom teraz** w panelu planu.

W wyniku uruchomienia planu replikacji replika maszyny wirtualnej pojawi się na liście **Wszystkie urządzenia** oznaczona następującą ikoną:

Testowanie repliki

Aby przygotować replikę do testu

1. Wybierz replikę do przetestowania.
2. Kliknij **Testuj replikę**.
3. Kliknij **Rozpocznij testowanie**.
4. Wybierz, czy włączona replika ma zostać podłączona do sieci. Domyślnie replika nie będzie podłączona do sieci.
5. [Opcjonalnie] Jeśli zdecydujesz się na podłączenie repliki do sieci, zaznacz pole wyboru **Zatrzymaj oryginalną maszynę wirtualną**, aby zatrzymać pierwotny komputer, zanim włączysz replikę.
6. Kliknij **Rozpocznij**.

Aby zatrzymać testowanie repliki

1. Wybierz testowaną replikę.
2. Kliknij **Testuj replikę**.
3. Kliknij **Zatrzymaj testowanie**.
4. Potwierdź decyzję.

© Acronis International GmbH, 2003-2024

Przełączanie awaryjne na replikę

Aby przełączyć maszynę awaryjnie na replikę

1. Wybierz replikę docelową przełączania awaryjnego.
2. Kliknij **Czynności dot. replik**.
3. Kliknij **Przełączanie awaryjne**.
4. Wybierz, czy włączona replika ma zostać podłączona do sieci. Domyślnie replika zostanie podłączona do tej samej sieci co pierwotna maszyna.
5. [Opcjonalnie] Jeśli zdecydujesz się na podłączenie repliki do sieci, wyczyść pole wyboru **Zatrzymaj oryginalną maszynę wirtualną**, aby utrzymać oryginalną maszynę w trybie online.
6. Kliknij **Rozpocznij**.

Gdy replika jest w stanie przełączania awaryjnego, możesz wybrać jedną z następujących czynności:

- **Zatrzymaj przełączanie awaryjne**

  Zatrzymaj przełączanie awaryjne, jeśli pierwotna maszyna została naprawiona. Replika zostanie wyłączona. Nastąpi wznowienie replikacji.
- **Wykonaj trwałe przełączenie awaryjne na replikę**

  Ta natychmiastowa operacja powoduje usunięcie flagi „replika" z maszyny wirtualnej, uniemożliwiając używanie tej maszyny jako lokalizacji docelowej replikacji. Jeśli zechcesz wznowić replikację, edytuj plan replikacji, wybierając tę maszynę jako źródło.
- **Powrót po awarii**

  W przypadku przełączenia awaryjnego na lokalizację, która nie jest przeznaczona do ciągłej obsługi operacji, wykonaj powrót po awarii. Replika zostanie odzyskana na pierwotną lub nową maszynę wirtualną. Po zakończeniu odzyskiwania na maszynę pierwotną maszyna ta zostanie włączona i nastąpi wznowienie replikacji. Jeśli zdecydujesz się na odzyskanie na nową maszynę, edytuj plan replikacji, wybierając tę maszynę jako źródło.

Zatrzymywanie przełączenia awaryjnego

Aby zatrzymać przełączanie awaryjne

1. Wybierz replikę znajdującą się w stanie przełączania awaryjnego.
2. Kliknij **Czynności dot. replik**.
3. Kliknij **Zatrzymaj przełączanie awaryjne**.
4. Potwierdź decyzję.

Wykonywanie trwałego przełączenia awaryjnego

Aby wykonać trwałe przełączenie awaryjne

1. Wybierz replikę znajdującą się w stanie przełączania awaryjnego.
2. Kliknij **Czynności dot. replik**.

© Acronis International GmbH, 2003-2024

3. Kliknij **Trwałe przełączenie awaryjne**.
4. [Opcjonalnie] Zmień nazwę maszyny wirtualnej.
5. [Opcjonalnie] Zaznacz pole wyboru **Zatrzymaj oryginalną maszynę wirtualną**.
6. Kliknij **Rozpocznij**.

Wykonywanie powrotu po awarii

Aby wykonać operację powrotu po awarii z repliki

1. Wybierz replikę znajdującą się w stanie przełączania awaryjnego.
2. Kliknij **Czynności dot. replik**.
3. Kliknij **Powrót po awarii z repliki**.
   Program automatycznie wybierze pierwotny komputer jako komputer docelowy.
4. [Opcjonalnie] Kliknij **Komputer docelowy**, a następnie zrób tak:
   a. Określ, czy chcesz wykonać powrót po awarii na nową, czy na już istniejącą maszynę.
   b. Wybierz host ESXi i określ nazwę nowej maszyny lub wybierz maszynę już istniejącą.
   c. Kliknij **OK**.
5. [Opcjonalnie] W przypadku wykonywania powrotu po awarii na nową maszynę możesz też zrobić tak:
   - Kliknij **Magazyn danych**, aby wybrać magazyn danych dla maszyny wirtualnej.
   - Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów oraz połączenia sieciowe maszyny wirtualnej.
6. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby zmodyfikować opcje powrotu po awarii.
7. Kliknij **Rozpocznij odzyskiwanie**.
8. Potwierdź decyzję.

Opcje replikacji

Aby zmodyfikować opcje replikacji, kliknij ikonę koła zębatego widoczną obok nazwy planu replikacji, a następnie kliknij **Opcje replikacji**.

CBT (Changed Block Tracking)

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Changed Block Tracking (CBT)".

Alokowanie dysków

Ta opcja umożliwia określenie ustawień alokowania dysków na potrzeby repliki.

Ustawienie wstępne: **Alokowanie elastyczne**.

Dostępne są następujące wartości: **Alokowanie elastyczne**, **Alokowanie nieelastyczne**, **Zachowaj pierwotne ustawienie**.

© Acronis International GmbH, 2003-2024

Obsługa błędów

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Obsługa błędów".

Polecenia poprzedzające/następujące

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Polecenia poprzedzające/następujące".

Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych".

Opcje powrotu po awarii

Aby zmodyfikować opcje powrotu po awarii, kliknij **Opcje odzyskiwania** podczas konfigurowania powrotu po awarii.

Obsługa błędów

Opcja ta jest podobna do opcji odzyskiwania „Obsługa błędów".

Wydajność

Opcja jest podobna do opcji odzyskiwania „Wydajność".

Polecenia poprzedzające/następujące

Opcja ta jest podobna do opcji odzyskiwania „Polecenia poprzedzające/następujące".

Zarządzanie zasilaniem maszyn wirtualnych

Opcja ta jest podobna do opcji odzyskiwania „Zarządzanie zasilaniem maszyn wirtualnych".

Seeding repliki początkowej

Aby przyspieszyć replikację do lokalizacji zdalnej i zmniejszyć obciążenie przepustowości sieci, można przeprowadzić seeding repliki.

Ważne
Aby można było wykonać seeding repliki, na docelowym hoście ESXi musi działać agent dla VMware (urządzenie wirtualne).

Aby przeprowadzić seeding repliki początkowej

1. Wykonaj jedną z następujących czynności:
   - Jeśli pierwotna maszyna wirtualna może zostać wyłączona, wyłącz ją i przejdź do kroku 4.
   - Jeśli pierwotna maszyna wirtualna nie może zostać wyłączona, przejdź do następnego kroku.
2. Utwórz plan replikacji.

© Acronis International GmbH, 2003-2024

Podczas tworzenia planu w polu **Komputer docelowy** wybierz **Nowa replika** oraz host ESXi, na którym znajduje się oryginalna maszyna.

3. Uruchom plan raz.

   Replika zostanie utworzona na pierwotnej maszynie ESXi.
4. Wyeksportuj pliki maszyny wirtualnej (lub repliki) na zewnętrzny dysk twardy.
   a. Podłącz zewnętrzny dysk twardy do komputera z działającym klientem vSphere.
   b. Połącz klienta vSphere z pierwotną maszyną vCenter\ESXi.
   c. Wybierz nowo utworzoną replikę w obszarze inwentaryzacji.
   d. Kliknij **Plik** > **Eksportuj** > **Eksportuj szablon OVF**.
   e. W polu **Katalog** określ folder na zewnętrznym dysku twardym.
   f. Kliknij **OK**.
5. Prześlij dysk twardy do lokalizacji zdalnej.
6. Zaimportuj replikę na docelową maszynę ESXi.
   a. Podłącz zewnętrzny dysk twardy do komputera z działającym klientem vSphere.
   b. Połącz klienta vSphere z docelową maszyną vCenter\ESXi.
   c. Kliknij **Plik** > **Wdróż szablon OVF**.
   d. W polu **Wdróż z pliku lub adresu URL** określ szablon wyeksportowany w kroku 4.
   e. Wykonaj procedurę importu.
7. Edytuj plan replikacji utworzony w kroku 2. W polu **Komputer docelowy** wybierz **Istniejąca już replika**, a następnie wybierz zaimportowaną replikę.

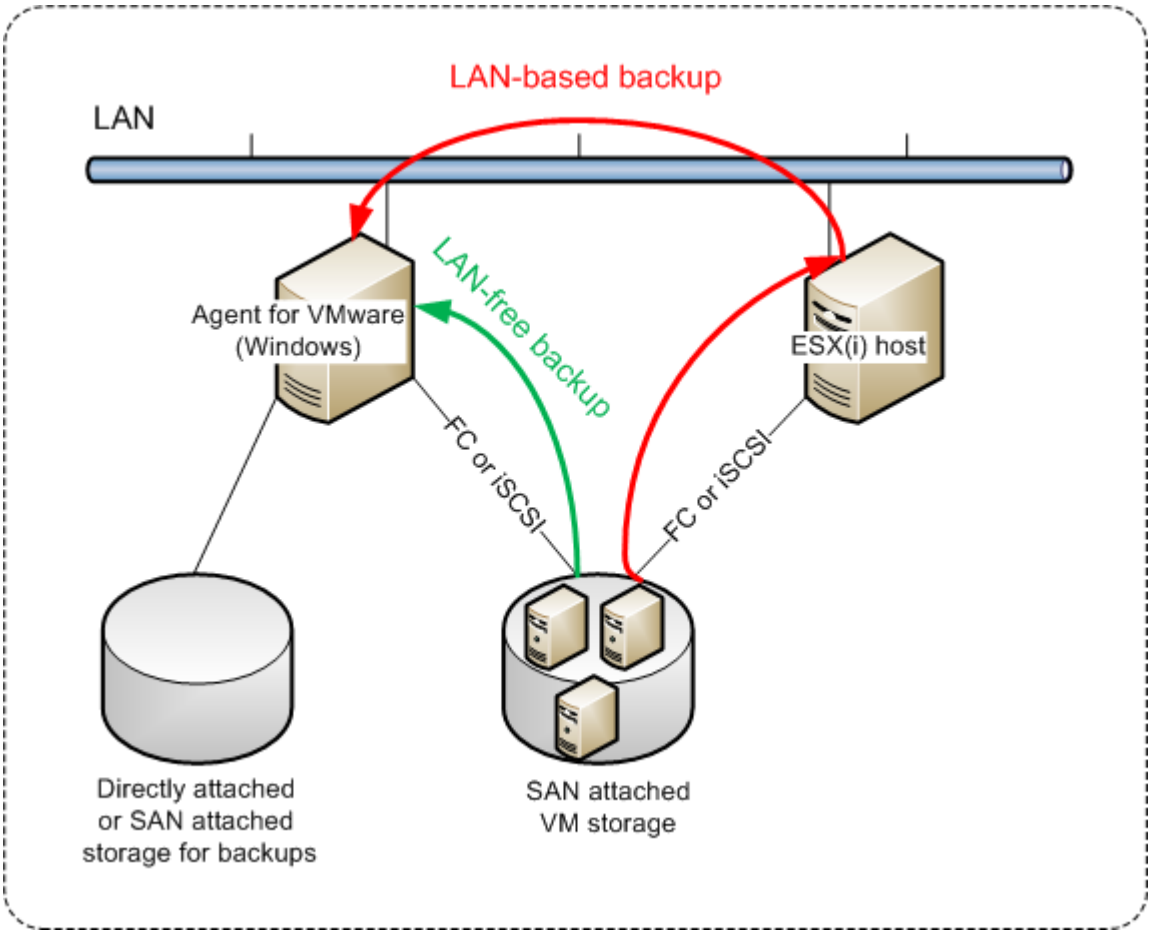
W wyniku tych działań oprogramowanie będzie nadal aktualizować replikę. Wszystkie replikacje będą przyrostowe.

Agent dla VMware — tworzenie kopii zapasowych bez obciążania sieci lokalnej

Jeśli system ESXi korzysta z pamięci masowej dołączonej do sieci SAN, zainstaluj agenta na komputerze podłączonym do tej samej sieci SAN. Agent będzie tworzył kopie zapasowe maszyn wirtualnych bezpośrednio z magazynu, a nie z hosta ESXi czy z sieci lokalnej. Funkcja ta jest nazywana tworzeniem kopii zapasowych bez obciążania sieci lokalnej.

Poniższa ilustracja przedstawia operację tworzenia kopii zapasowych opartego na sieci lokalnej oraz bez obciążania sieci lokalnej. Dostęp do maszyn wirtualnych z pominięciem sieci lokalnej jest możliwy w przypadku korzystania z łącza Fibre Channel (FC) lub sieci iSCSI Storage Area Network. Aby całkowicie wyeliminować konieczność przesyłania danych uwzględnianych w kopiach zapasowych przez sieć lokalną, przechowuj kopie zapasowe na dysku lokalnym komputera agenta lub na dołączonym magazynie SAN.

© Acronis International GmbH, 2003-2024



Aby umożliwić agentowi bezpośredni dostęp do magazynu danych

1. Zainstaluj agenta dla VMware na komputerze z systemem Windows, który ma dostęp przez sieć do serwera vCenter.
2. Podłącz do tego komputera jednostkę LUN zawierającą magazyn danych. Uwzględnij następujące wskazówki:
   - Użyj tego samego protokołu (np. iSCSI lub FC), którego używa połączenie magazynu danych z hostem ESXi.
   - *Nie wolno* zainicjować jednostki LUN i musi ona być widoczna w narzędziu **Zarządzanie dyskami** jako dysk „offline”. Jeśli system Windows zainicjuje jednostkę LUN, może ona ulec uszkodzeniu i środowisko VMware vSphere nie będzie mogło jej odczytać.

W związku z tym agent użyje trybu transportu SAN, aby uzyskać dostęp do dysków wirtualnych, tj. odczyta surowe sektory jednostki LUN przez interfejs iSCSI/FC bez rozpoznania systemu plików VMFS (o którym system Windows nie otrzymuje informacji).

Ograniczenia

- W środowisku vSphere w wersji 6.0 lub nowszej agent nie może korzystać z trybu transportu SAN, jeśli część dysków maszyny wirtualnej znajduje się na woluminie wirtualnym VMware Virtual Volume (VMware Virtual Volume — VVol), a część nie. Utworzenie kopii zapasowej takich maszyn wirtualnych się nie powiedzie.

© Acronis International GmbH, 2003-2024

- Kopie zapasowe szyfrowanych maszyn wirtualnych (takie maszyny wprowadzono w środowisku VMware vSphere 6.5) zostaną utworzone przy użyciu sieci lokalnej nawet w przypadku skonfigurowania dla agenta trybu transportu SAN. Ponieważ środowisko VMware nie obsługuje tworzenia kopii zapasowych zaszyfrowanych dysków wirtualnych w trybie transportu SAN, agent wykona przełączenie awaryjne na tryb transportu NBD.

Przykład

Jeśli korzystasz z technologii iSCSI SAN, skonfiguruj inicjator iSCSI na komputerze z systemem Windows i zainstalowanym agentem dla VMware.

Aby skonfigurować zasady SAN

1. Zaloguj się jako administrator, otwórz wiersz polecenia, wpisz `diskpart`, a następnie naciśnij **Enter**.
2. Wpisz `san`, a następnie naciśnij **Enter**. Upewnij się, że jest wyświetlana opcja **Zasady SAN: Wszystkie offline**.
3. Jeśli jest ustawiona inna wartość zasad SAN:
   a. Wpisz `san policy=offlineall`.
   b. Naciśnij **Enter**.
   c. Aby sprawdzić, czy ustawienia zostały poprawnie zastosowane, wykonaj krok 2.
   d. Uruchom ponownie komputer.

Aby skonfigurować inicjator iSCSI

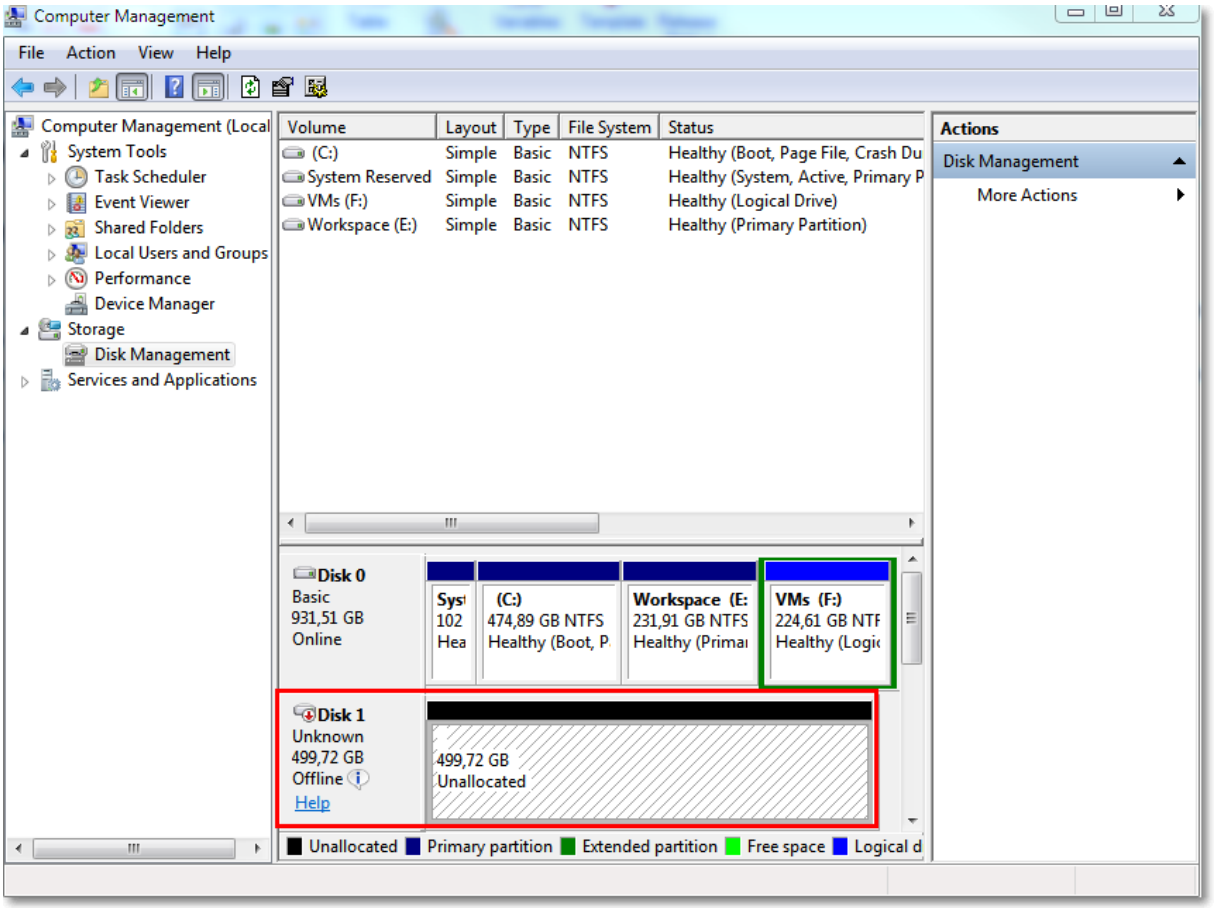
1. Przejdź do sekcji **Panel sterowania** > **Narzędzia administracyjne** > **Inicjator iSCSI**.

   Uwaga
   Aby znaleźć aplet **Narzędzia administracyjne**, być może trzeba będzie zmienić widok w **Panelu sterowania** na inny niż **Narzędzia główne** czy **Kategoria** albo skorzystać z funkcji wyszukiwania.

2. Jeśli inicjator Microsoft iSCSI jest uruchamiany po raz pierwszy, potwierdź, że chcesz uruchomić usługę inicjatora iSCSI firmy Microsoft.
3. Na karcie **Miejsca docelowe** wpisz w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP docelowego urządzenia SAN, a następnie kliknij **Quick Connect**.
4. Wybierz jednostkę LUN, na której znajduje się magazyn danych, a następnie kliknij **Połącz**.
   Jeśli jednostka LUN nie jest wyświetlana, upewnij się, że podział na strefy obiektu docelowego iSCSI umożliwia komputerowi z uruchomionym agentem dostęp o tej jednostki LUN. Komputer musi zostać dodany do listy dozwolonych inicjatorów iSCSI na tym obiekcie docelowym.
5. Kliknij **OK**.

Gotowa jednostka LUN sieci SAN powinna się pojawić w obszarze **Zarządzanie dyskami**, tak jak pokazano na poniższym zarzucie ekranu.

© Acronis International GmbH, 2003-2024



Używanie magazynu dołączonego lokalnie

Do agenta dla VMware (urządzenie wirtualne) można dołączyć dodatkowy dysk pełniący funkcję magazynu dołączonego lokalnie, w którym agent może przechowywać kopie zapasowe. Takie rozwiązanie eliminuje ruch sieciowy między agentem a lokalizacją kopii zapasowych.

Urządzenie wirtualne, które działa na tym samym hoście lub w tym samym klastrze co maszyny wirtualne uwzględniane w kopiach zapasowych, ma bezpośredni dostęp do magazynów danych, w których znajdują się te maszyny. Oznacza to, że urządzenie może podłączyć dyski uwzględniane w kopiach zapasowych przy użyciu transportu HotAdd, w związku z czym ruch związany z tworzeniem kopii zapasowych jest kierowany z jednego dysku lokalnego na drugi. Jeśli magazyn danych jest podłączony jako **Dysk/jednostka LUN**, a nie folder **NFS**, operacja tworzenia kopii zapasowej zostanie wykonana bez korzystania z sieci lokalnej. W przypadku magazynu danych NFS wystąpi ruch sieciowy między nim a hostem.

Użycie magazynu dołączonego lokalnie oznacza, że agent będzie zawsze tworzył kopie zapasowe tych samych komputerów. Jeśli w środowisku vSphere jest uruchomionych wiele agentów, a co najmniej jeden z nich używa magazynów dołączonych lokalnie, należy ręcznie powiązać każdego agenta ze wszystkimi komputerami, których kopie zapasowe ma on tworzyć. W innym przypadku, jeśli komputery są rozdzielone pomiędzy agenty przez serwer zarządzania, kopie zapasowe jednego komputera mogą być rozproszone w wielu magazynach.

© Acronis International GmbH, 2003-2024

Program umożliwia dodanie magazynu do już działającego agenta lub wykonanie tego w trakcie wdrażania agenta z szablonu OVF.

Aby dołączyć magazyn do już działającego agenta

1. W widoku inwentaryzacji serwera VMware vSphere kliknij prawym przyciskiem myszy opcję Agent dla VMware (urządzenie wirtualne).
2. Dodaj dysk, edytując ustawienia maszyny wirtualnej. Dysk nie może być mniejszy niż 10 GB.

   Ostrzeżenie!
   Dodając już istniejący dysk, zachowaj ostrożność. Po utworzeniu magazynu wszystkie dane zawarte dotychczas na tym dysku zostaną utracone.

3. Przejdź do konsoli urządzenia wirtualnego. W dolnej części ekranu jest dostępne łącze **Utwórz magazyn**. Jeśli go tam nie ma, kliknij opcję **Odśwież**.
4. Kliknij łącze **Utwórz magazyn**, wybierz dysk i określ jego etykietę. Z powodu ograniczeń systemu plików etykieta może mieć długość maksymalnie 16 znaków.

Aby wybrać magazyn dołączony lokalnie jako miejsce docelowe kopii zapasowej

- Podczas tworzenia planu ochrony w sekcji **Miejsce docelowe kopii zapasowej** wybierz opcję **Foldery lokalne**, a następnie wpisz literę magazynu dołączonego lokalnie, na przykład **D:**.

Uwaga
Magazyn dołączany lokalnie (Locally Attached Storage, LAS) jest przeznaczony do stosunkowo małych środowisk z jednym agentem (urządzeniem wirtualnym). Przetestowaliśmy magazyny dołączone lokalnie o pojemności do 5 TB. Można podłączać większe dyski na własne ryzyko, ale takie konfiguracje nie są oficjalnie obsługiwane. Jeśli dane kopii zapasowej zajmują więcej niż 5 TB, zalecamy użycie innego typu pamięci masowej. Można na przykład utworzyć dysk wirtualny VMware i podłączyć go do dowolnej maszyny wirtualnej oraz utworzyć na nim udział sieciowy, który będzie następnie służyć jako miejsce docelowe kopii zapasowych zamiast urządzenia LAS.

Wiązanie maszyn wirtualnych

W tej sekcji wyjaśniono, jak usługa Cyber Protection organizuje pracę wielu agentów na serwerze VMware vCenter.

Poniższy algorytm dystrybucji dotyczy zarówno urządzeń wirtualnych, jak i agentów zainstalowanych w systemie Windows.

Algorytm dystrybucji

Maszyny wirtualne są automatycznie równomiernie rozprowadzane między agentami dla VMware. Równomiernie oznacza, że każdy agent obsługuje tę samą liczbę komputerów. Rozmiar powierzchni magazynu zajęty przez maszynę wirtualną nie jest obliczany.

Jednak przy wybieraniu agenta dla maszyny program próbuje optymalizować ogólną wydajność systemu. Program uwzględnia w szczególności lokalizację agenta i maszyny wirtualnej. Preferowany

© Acronis International GmbH, 2003-2024

jest agent z tego samego hosta. W przypadku braku agenta na tym samym hoście, wybierany jest agent z tego samego klastra.

Po przypisaniu maszyny wirtualnej do agenta wszystkie kopie zapasowe tej maszyny będą delegowane do tego agenta.

Redystrybucja

Do redystrybucji dochodzi za każdym razem, kiedy załamuje się ustalona równowaga, a dokładniej, kiedy nierównowaga obciążenia między agentami przekracza 20 procent. Taka sytuacja może mieć miejsce w przypadku dodania lub usunięcia komputera albo agenta, migracji komputera do innego hosta lub klastra, lub w przypadku ręcznego powiązania komputera z agentem. W takim przypadku usługa Cyber Protection ponownie odpowiednio przydzieli poszczególne komputery przy użyciu tego samego algorytmu.

Przykład: zauważasz potrzebę podłączenia większej liczby agentów w celu zwiększenia przepustowości i wdrażasz w klastrze dodatkowe urządzenie wirtualne. Usługa Cyber Protection przypisze nowemu agentowi najbardziej odpowiednie komputery. Zmniejszy się obciążenie starszych agentów.

W przypadku usunięcia agenta z usługi Cyber Protection komputery przypisane temu agentowi zostaną przydzielone pozostałym agentom. Nie będzie to jednak mieć miejsca w przypadku uszkodzenia agenta lub jego ręcznego usunięcia ze środowiska vSphere. Proces redystrybucji rozpocznie się dopiero po usunięciu takiego agenta z interfejsu internetowego.

Obserwacja wyniku redystrybucji

Można sprawdzić wynik automatycznej dystrybucji:

- w kolumnie **Agent** dla każdej maszyny wirtualnej w sekcji **Wszystkie urządzenia**;
- w sekcji **Przypisane maszyny wirtualne** panelu **Szczegóły**, kiedy agent jest wybrany w sekcji **Ustawienia** > **Agenci**

Powiązanie ręczne

Powiązanie agenta dla VMware umożliwia wykluczenie maszyny wirtualnej z tego procesu rozdzielania przez określenie agenta, który musi zawsze wykonywać kopie zapasowe tej maszyny. Jest zachowywana ogólna równowaga, ale dana maszyna może zostać przekazana do innego agenta tylko pod warunkiem, że pierwotny agent zostanie usunięty.

Aby powiązać maszynę z agentem

1. Wybierz maszynę.
2. Kliknij opcję **Szczegóły**.
   W sekcji **Przypisany agent** program wyświetla agenta zarządzającego obecnie wybraną maszyną.
3. Kliknij przycisk **Zmień**.

© Acronis International GmbH, 2003-2024

4. Wybierz opcję **Ręcznie**.
5. Wybierz agenta, z którym chcesz powiązać maszynę.
6. Kliknij **Zapisz**.

Aby usunąć powiązanie maszyny z agentem

1. Wybierz maszynę.
2. Kliknij opcję **Szczegóły**.
   W sekcji **Przypisany agent** program wyświetla agenta zarządzającego obecnie wybraną maszyną.
3. Kliknij przycisk **Zmień**.
4. Wybierz opcję **Automatycznie**.
5. Kliknij **Zapisz**.

Wyłączanie automatycznego przypisywania do agenta

Można wyłączyć automatyczne przypisywanie do agenta dla VMware, aby wykluczyć go z procesu dystrybucji. W tym celu należy określić listę maszyn, których kopie zapasowe musi wykonywać ten agent. Zostanie zachowana ogólna równowaga między agentami.

Nie można wyłączyć automatycznego przypisywania do agenta, jeśli nie ma innych zarejestrowanych agentów lub wyłączono automatyczne przypisywanie do wszystkich pozostałych agentów.

Aby wyłączyć automatyczne przypisywanie do agenta

1. Kliknij **Ustawienia** > **Agenty**.
2. Wybierz agenta dla VMware, w przypadku którego chcesz wyłączyć automatyczne przypisywanie.
3. Kliknij opcję **Szczegóły**.
4. Wyłącz przełącznik **Przypisanie automatyczne**.

Przykłady użycia

- Ręczne powiązanie jest przydatne, kiedy trzeba uwzględnić konkretną (bardzo dużą) maszynę podczas tworzenia kopii zapasowych przez agenta dla VMware (Windows) za pośrednictwem łącza Fibre Channel, podczas gdy pozostałe maszyny mają być uwzględniane w tworzeniu kopii przez urządzenia wirtualne.
- Jeśli agent ma magazyn dołączony lokalnie, należy powiązać maszyny wirtualne z agentem.
- Wyłączenie automatycznego przypisywania umożliwia zagwarantowanie przewidywalnego tworzenia kopii zapasowych konkretnej maszyny zgodnie z określonym harmonogramem. W zaplanowanym czasie agent tworzący kopie zapasowe tylko jednej maszyny wirtualnej nie może być zajęty tworzeniem kopii zapasowych innych maszyn wirtualnych.
- Wyłączenie automatycznego przypisywania jest przydatne, kiedy istnieje wiele hostów ESXi w różnych lokalizacjach geograficznych. Jeśli automatyczne przypisywanie zostanie wyłączone, a maszyny wirtualne z poszczególnych hostów zostaną powiązane z agentami uruchomionymi na

© Acronis International GmbH, 2003-2024

tych samych hostach, można zagwarantować, że agent nigdy nie będzie tworzyć kopii zapasowych maszyn uruchomionych na zdalnych hostach ESXi. Pozwoli to ograniczyć ruch sieciowy.

Automatyczne uruchamianie skryptów poprzedzających zablokowanie i następujących po odblokowaniu

Za pomocą narzędzi VMware Tools można automatycznie uruchamiać niestandardowe skrypty poprzedzające zablokowanie i następujące po odblokowaniu na maszynach wirtualnych, których kopie zapasowe są tworzone w trybie bezagentowym. Dzięki temu można na przykład uruchamiać niestandardowe skrypty wyciszania i tworzyć kopie zapasowe spójne z aplikacjami w przypadku maszyn wirtualnych zawierających aplikacje, które nie uwzględniają usługi VSS.

Wymagania wstępne

Skrypty poprzedzające zablokowanie i następujące po odblokowaniu muszą się znajdować w określonym folderze na maszynie wirtualnej.

- W przypadku maszyn wirtualnych z systemem Windows lokalizacja tego folderu zależy od wersji środowiska ESXi hosta.

  Na przykład w przypadku maszyn wirtualnych działających na hoście ESXi 6.5 jest to folder `C:\Program Files\VMware\VMware Tools\backupScripts.d\`. Trzeba ręcznie utworzyć folder `backupScritps.d`. Nie należy przechowywać w tym folderze plików innego typu, ponieważ może to skutkować niestabilnym działaniem narzędzi VMware Tools.

  Więcej informacji na temat lokalizacji skryptów poprzedzających zablokowanie i następujących po odblokowaniu dla innych wersji hostów ESXi można znaleźć w dokumentacji firmy VMware.
- W przypadku maszyn wirtualnych z systemem Linux skopiuj skrypty odpowiednio do katalogów `/usr/sbin/pre-freeze-script` i `/usr/sbin/post-thaw-script`. Skrypty z katalogu `/usr/sbin/pre-freeze-script` są uruchamiane podczas tworzenia migawki, a skrypty z katalogu `/usr/sbin/post-thaw-script` są uruchamiane po ukończeniu migawki. Skrypty muszą być dostępne do wykonywania przez użytkownika narzędzi VMware Tools.

Aby włączyć automatyczne uruchamianie skryptów poprzedzających zablokowanie i następujących po odblokowaniu

1. Upewnij się, że na maszynie wirtualnej są zainstalowane narzędzia VMware Tools.
2. Na maszynie wirtualnej umieść skrypty niestandardowe w wymaganym folderze.
3. W planie ochrony tej maszyny włącz opcję **Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych**.

   Spowoduje to utworzenie migawki środowiska VMware z włączoną opcją **Wycisz system plików gościa**, co z kolei wyzwala skrypty poprzedzające zablokowanie i następujące po odblokowaniu w ramach maszyny wirtualnej.

Na maszynach wirtualnych z aplikacjami uwzględniającymi usługę VSS, takimi jak Microsoft SQL Server czy Microsoft Exchange, nie trzeba uruchamiać niestandardowych skryptów wyciszania. Aby

© Acronis International GmbH, 2003-2024

utworzyć kopię zapasową spójną z aplikacjami w przypadku takich maszyn, włącz w planie ochrony opcję **Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych**.

Obsługa migracji maszyn wirtualnych

Ta sekcja zawiera informacje, czego należy się spodziewać w przypadku migracji maszyn wirtualnych w środowisku vSphere, w tym migracji między hostami ESXi wchodzącymi w skład klastra vSphere.

Narzędzie vMotion umożliwia przeniesienie stanu i konfiguracji maszyny wirtualnej na inny host, podczas gdy dyski maszyny pozostają w tej samej lokalizacji w magazynie współużytkowanym. Narzędzie Storage vMotion umożliwia przeniesienie dysków maszyny wirtualnej do innego magazynu danych.

- Migracja dokonywana za pomocą narzędzia vMotion, w tym Storage vMotion, nie jest obsługiwana w przypadku maszyny wirtualnej, na której działa agent dla VMware (urządzenie wirtualne) i jest automatycznie wyłączana. Ta maszyna wirtualna jest dodawana do listy **Zastępowanie maszyn wirtualnych** w konfiguracji klastra vSphere.
- Kiedy rozpoczyna się tworzenie kopii zapasowej maszyny wirtualnej, migracja za pomocą narzędzia vMotion, w tym Storage vMotion, jest automatycznie wyłączana. Ta maszyna wirtualna jest na jakiś czas dodawana do listy **Zastępowanie maszyn wirtualnych** w konfiguracji klastra vSphere. Po zakończeniu tworzenia kopii zapasowej ustawienia z listy **Zastępowanie maszyn wirtualnych** są automatycznie przywracane do poprzedniego stanu.
- Tworzenie kopii zapasowej nie może się rozpocząć, jeśli trwa migracja maszyny wirtualnej za pomocą narzędzia vMotion, w tym Storage vMotion. Tworzenie kopii zapasowej tej maszyny rozpocznie się po zakończeniu jej migracji.

Ochrona środowisk wirtualizacji

W konsoli Cyber Protect można przeglądać środowiska vSphere, Hyper-V i Virtuozzo w ich macierzystej prezentacji. Po zainstalowaniu i zarejestrowaniu odpowiedniego agenta w obszarze Urządzenia będzie widoczna karta **VMware**, **Hyper-V** lub **Virtuozzo**.

Na przykład na karcie **VMware** można tworzyć kopie zapasowe następujących obiektów infrastruktury vSphere:

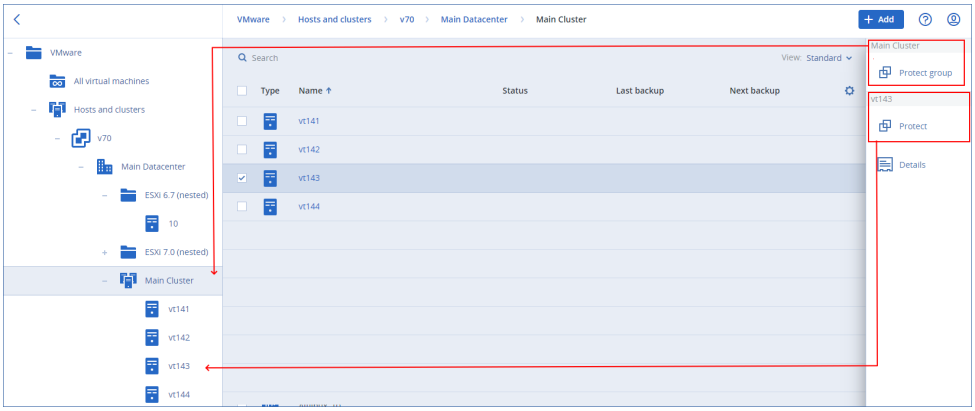
- vCenter
- Centrum danych
- Folder
- Klaster
- Host ESXi
- Pula zasobów
- Maszyna wirtualna

© Acronis International GmbH, 2003-2024

Aby zastosować plan do wybranego obiektu infrastruktury, kliknij **Chroń**. W kopiach zapasowych będą uwzględniane wszystkie obiekty podrzędne.

Aby zastosować plan do obiektu nadrzędnego wybranego obiektu infrastruktury, kliknij **Chroń grupę**. W kopiach zapasowych będą uwzględniane wszystkie obiekty podrzędne obiektu nadrzędnego.

Jeśli na przykład zastosujesz plan do hosta ESXi, w kopiach zapasowych będą uwzględniane wszystkie maszyny wirtualne działające na tym hoście. Jeśli zastosujesz plan do klastra nadrzędnego, w kopiach zapasowych będą uwzględniane wszystkie maszyny wirtualne działające na wszystkich hostach w tym klastrze.



Wyświetlanie statusu kopii zapasowej w kliencie vSphere

W kliencie vSphere można wyświetlić status kopii zapasowej i czas utworzenia ostatniej kopii zapasowej maszyny wirtualnej.

Informacje te są wyświetlane w podsumowaniu maszyny wirtualnej (**Podsumowanie** > **Atrybuty niestandardowe** / **Adnotacje** / **Uwagi**, w zależności od typu klienta i wersji środowiska vSphere). Można również włączyć kolumny **Ostatnia kopia zapasowa** i **Status kopii zapasowej** na karcie **Maszyny wirtualne** w przypadku dowolnego hosta, centrum danych, folderu, puli zasobów lub całego serwera vCenter.

Aby można było podać te atrybuty, agent dla VMware musi mieć następujące uprawnienia — oprócz tych opisanych w sekcji „Agent dla VMware — niezbędne uprawnienia”:

- **Globalne** > **Zarządzaj atrybutami niestandardowymi**
- **Globalne** > **Ustaw atrybut niestandardowy**

Wymagane uprawnienia dla agenta dla VMware

Uwaga
Aby włączyć tworzenie kopii zapasowych maszyn wirtualnych, zainstaluj interfejsy API vStorage na hoście ESXi. Więcej informacji można znaleźć w tym artykule bazy wiedzy Knowledge Base.

© Acronis International GmbH, 2003-2024

Agent dla VMware uwierzytelnia się na serwerze vCenter lub hoście ESXi przy użyciu konta użytkownika określonego podczas wdrażania agenta. Konto użytkownika musi mieć rolę obejmującą uprawnienia wymienione w poniższej tabeli. Zalecamy korzystanie ze specjalnego konta i roli, a nie z już istniejącego konta z rolą Administrator.

Konto użytkownika musi mieć przyznane uprawnienia dostępu do wszystkich poziomów infrastruktury vSphere, takich jak vCenter, centra danych, klastry, hosty ESXi, pule zasobów i maszyny wirtualne. Aby się dowiedzieć, jak dodać uprawnienie na poziomie serwera vCenter i propagować je na inne poziomy, zobacz sekcję "Przyznawanie uprawnień dostępu do konta użytkownika" (s. 750).

Konto użytkownika używane przez agenta dla VMware można zmienić bez ponownego wdrażania agenta. Aby się dowiedzieć, jak zmienić konto, zobacz sekcję "Zmienianie konta użytkownika dla agenta dla VMware" (s. 751).

Obiekt	Uprawnienie	Operacja			
		Utworzenie kopii zapasowej maszyny wirtualnej	**Odzyskanie na nową maszynę wirtualną**	**Odzyskanie na istniejącą maszynę wirtualną**	**Uruchom maszynę wirtualną z kopii zapasowej**
Operacje kryptograficzne (począwszy od vSphere 6.5)					
	Dodaj dysk	+*			
	Dostęp bezpośredni	+*			
Magazyn danych					
	Przydzielenie miejsca		+	+	+
	Przeglądanie magazynu danych				+
	Konfigurowanie magazynu danych	+	+	+	+
	Niskopoziomowe				+

© Acronis International GmbH, 2003-2024

Obiekt	Uprawnienie	Operacja			
		Utworzenie kopii zapasowej maszyny wirtualnej	Odzyskanie na nową maszynę wirtualną	Odzyskanie na istniejącą maszynę wirtualną	Uruchom maszynę wirtualną z kopii zapasowej
	operacje na plikach				
Globalne					
	Metody wyłączania	+	+	+	
	Metody włączania	+	+	+	
	Licencje	+	+	+	+
	Zarządzaj atrybutami niestandardowymi	+	+	+	
	Ustaw atrybut niestandardowy	+	+	+	
Host > Konfiguracja					
	Konfiguracja partycji magazynu				+
	Modyfikowanie klastra				
Host > Operacje lokalne					
	Utwórz maszynę wirtualną				+
	Usuń maszynę wirtualną				+
	Skonfiguruj ponownie				+

© Acronis International GmbH, 2003-2024

Obiekt	Uprawnienie	Operacja			
		Utworzenie kopii zapasowej maszyny wirtualnej	Odzyskanie na nową maszynę wirtualną	Odzyskanie na istniejącą maszynę wirtualną	Uruchom maszynę wirtualną z kopii zapasowej
	maszynę wirtualną				
Sieć					
	Przypisanie sieci		+	+	+
Zasób					
	Przypisz maszynę wirtualną do puli zasobów		+	+	+
Maszyna wirtualna > **Zmień konfigurację**					
	Wykup dzierżawę dysku	+		+	
	Dodanie istniejącego dysku	+	+		+
	Dodaj nowy dysk		+	+	+
	Dodanie lub usunięcie urządzenia		+		+
	Konfiguracja zaawansowana	+	+	+	
	Zmiana liczby procesorów		+		
	Zmień pamięć		+		
	Zmień ustawienia		+	+	+
	Zmień zasób	+	+		

© Acronis International GmbH, 2003-2024

Obiekt	Uprawnienie	Operacja			
		Utworzenie kopii zapasowej maszyny wirtualnej	**Odzyskanie na nową maszynę wirtualną**	**Odzyskanie na istniejącą maszynę wirtualną**	**Uruchom maszynę wirtualną z kopii zapasowej**
	Modyfikuj ustawienia urządzeń	+	+		
	Usunięcie dysku	+	+	+	+
	Zmień nazwę		+		
	Ustaw adnotację				+
	Przełącz śledzenie zmian na dysku	+		+	
Maszyna wirtualna > **Operacje gościa**					
	Modyfikacje operacji gościa	+**			
	Wykonanie programu obsługi gościa	+**			
	Zapytania operacji gościa	+**			
Maszyna wirtualna > **Interakcja**					
	Uzyskaj bilet kontroli gościa (w środowisku vSphere 4.1 i 5.0)				+
	Konfiguracja nośnika CD		+	+	
	Zarządzanie systemem				+

© Acronis International GmbH, 2003-2024

Obiekt	Uprawnienie	Operacja			
		Utworzenie kopii zapasowej maszyny wirtualnej	**Odzyskanie na nową maszynę wirtualną**	**Odzyskanie na istniejącą maszynę wirtualną**	**Uruchom maszynę wirtualną z kopii zapasowej**
	operacyjnym-gościem za pośrednictwem interfejsu API VIX (w środowisku vSphere w wersji 5.1 lub nowszej)				
	Wyłączenie zasilania			+	+
	Włączenie zasilania		+	+	+
Maszyna wirtualna > **Inwentaryzacja**					
	Utworzenie na podstawie istniejącej		+	+	+
	Utwórz nowy		+	+	+
	Rejestruj				+
	Usuń		+	+	+
	Wyrejestruj				+
Maszyna wirtualna > **Alokowanie**					
	Zezwolenie na dostęp do dysku		+	+	+
	Zezwól na dostęp do dysku w trybie tylko do odczytu	+		+	

© Acronis International GmbH, 2003-2024

Obiekt	Uprawnienie	Operacja			
		Utworzenie kopii zapasowej maszyny wirtualnej	**Odzyskanie na nową maszynę wirtualną**	**Odzyskanie na istniejącą maszynę wirtualną**	**Uruchom maszynę wirtualną z kopii zapasowej**
	Zezwolenie na pobranie maszyny wirtualnej	+	+	+	+
Maszyna wirtualna > **Stan** **Maszyna wirtualna** > **Zarządzanie migawkami** (środowisko vSphere 6.5 lub nowsze)					
	Utworzenie migawki	+		+	+
	Usunięcie migawki	+		+	+
vApp					
	Dodaj maszynę wirtualną				+

***** To uprawnienie jest wymagane tylko w przypadku tworzenia kopii zapasowych zaszyfrowanych komputerów.

****** To uprawnienie jest wymagane tylko w przypadku tworzenia kopii zapasowych uwzględniających aplikacje.

Przyznawanie uprawnień dostępu do konta użytkownika

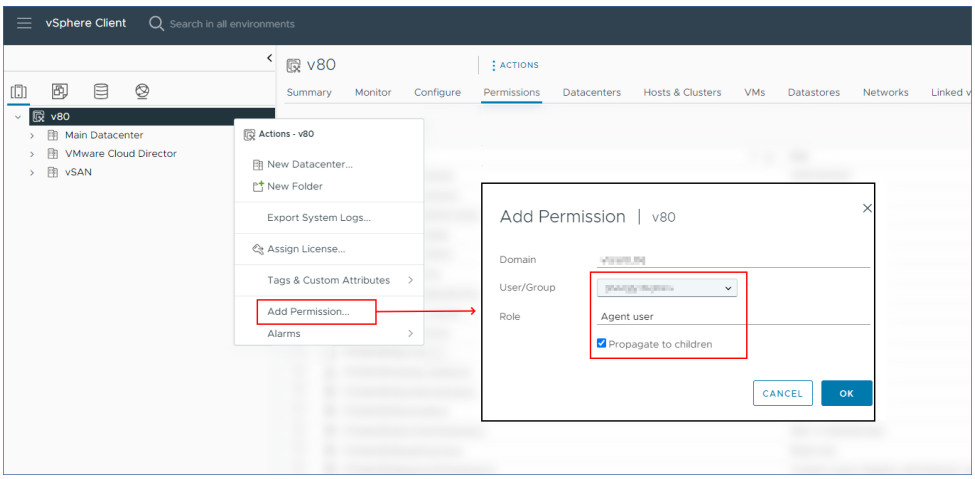
Konto użytkownika używane przez agenta dla VMware musi mieć dostęp do wszystkich poziomów infrastruktury vSphere, takich jak vCenter, centra danych, klastry, hosty ESXi, pule zasobów i maszyny wirtualne.

Aby przyznać uprawnienia dostępu do konta użytkownika

© Acronis International GmbH, 2003-2024

1. W kliencie vSphere przejdź do sekcji **Inventory** (Inwentaryzacja).
2. Kliknij prawym przyciskiem myszy obiekt **vCenter**, któremu chcesz przyznać uprawnienia, a następnie kliknij **Add Permission** (Dodaj uprawnienia).
3. W oknie dialogowym **Add Permission** (Dodaj uprawnienia) wybierz konto użytkownika i rolę.

   Rola musi obejmować uprawnienia wymienione w sekcji "Wymagane uprawnienia dla agenta dla VMware" (s. 744).
4. Zaznacz pole wyboru **Propagate to children** (Propaguj na elementy podrzędne).
5. Kliknij **OK**.



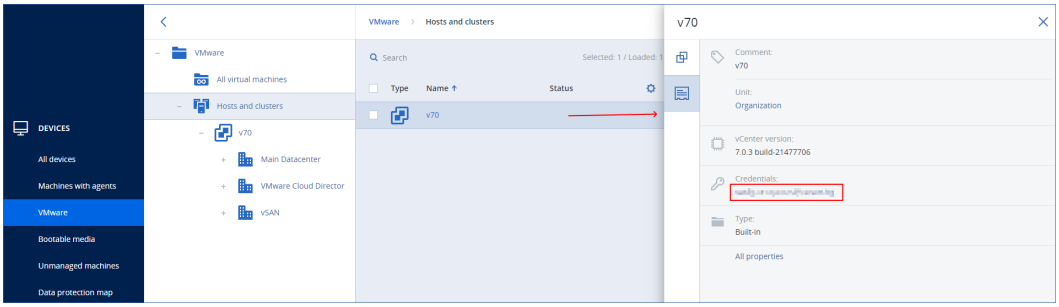
Zmienianie konta użytkownika dla agenta dla VMware

W konsoli Cyber Protect można zmienić konto użytkownika dla wybranego agenta lub wszystkich agentów w środowisku vCenter lub na hoście ESXi.

Aby zmienić konto użytkownika dla agenta dla VMware

Dla wszystkich agentów

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **VMware**.
2. Kliknij **Hosty i klastry**.
3. W panelu głównym kliknij puste miejsce obok nazwy serwera vCenter lub autonomicznego hosta ESXi.
4. W prawym panelu kliknij **Szczegóły**.
5. W sekcji **Poświadczenia** kliknij konto użytkownika.



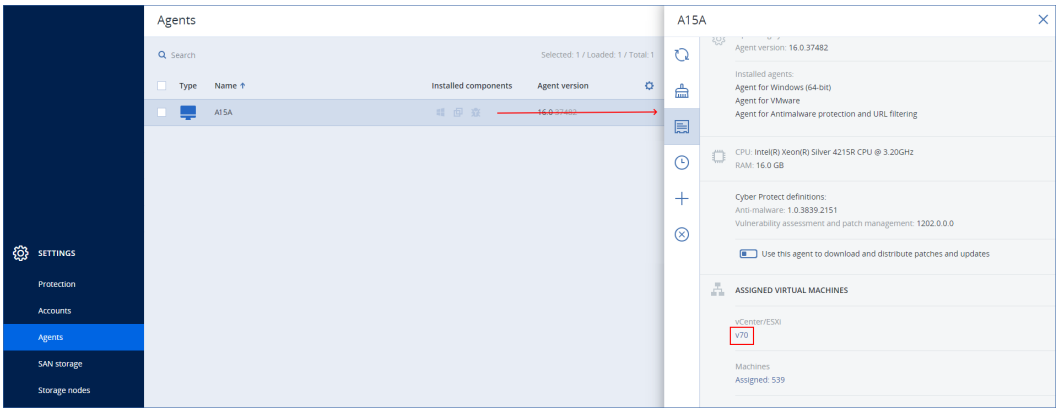
© Acronis International GmbH, 2003-2024

6. Określ nowe konto użytkownika i hasło do tego konta.
7. Kliknij **OK**.

W wyniku tych działań wszystkie agenty na tym serwerze vCenter lub hoście ESXi będą korzystać z nowego konta użytkownika.

Dla wybranego agenta

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Wybierz agenta.
3. W prawym panelu kliknij **Szczegóły**.
4. W obszarze **Przypisane maszyny wirtualne** kliknij nazwę vCenter/ESXi.



5. Na ekranie **Określ host VMware vCenter lub ESXi** określ nowe konto użytkownika i hasło do tego konta.
6. Kliknij **Konfiguruj**.

Tworzenie kopii zapasowych maszyn Hyper-V w klastrach

W przypadku klastrów Hyper-V maszyny wirtualne mogą migrować między węzłami klastra. Aby poprawnie skonfigurować tworzenie kopii zapasowych maszyn Hyper-V w klastrach, postępuj zgodnie z następującymi zaleceniami:

1. Maszyna musi być dostępna do tworzenia kopii zapasowych bez względu na węzeł, do którego migruje. Aby zapewnić agentowi dla Hyper-V dostęp do maszyny znajdującej się w dowolnym węźle, usługa agenta musi być uruchomiona na koncie użytkownika domeny z uprawnieniami administracyjnymi na każdym węźle klastra.

   Zaleca się określenie takiego konta dla usługi agenta podczas instalacji agenta dla Hyper-V.
2. Zainstaluj agenta dla Hyper-V w każdym węźle klastra.
3. Zarejestruj wszystkie agenty w usłudze Cyber Protection.

Wysoka dostępność odzyskanej maszyny

W przypadku odzyskiwania dysków z kopii zapasowej na już *istniejącą* maszynę wirtualną Hyper-V jej właściwość Wysoka dostępność pozostanie niezmieniona.

© Acronis International GmbH, 2003-2024

W przypadku odzyskiwania dysków z kopii zapasowej na *nową* maszynę wirtualną Hyper-V wynikowa maszyna nie będzie się cechowała wysoką dostępnością. Będzie ona traktowana jako maszyna zapasowa i będzie normalnie wyłączona. Jeśli wymagane jest użycie maszyny w środowisku produkcyjnym, można skonfigurować jej wysoką dostępność za pomocą przystawki **Zarządzanie klastrem awaryjnym**.

Ograniczanie łącznej liczby maszyn wirtualnych, których kopie zapasowe mogą być tworzone w tym samym czasie

W ramach opcji tworzenia kopii zapasowych **Tworzenie harmonogramu** można ograniczyć liczbę maszyn wirtualnych, których kopie zapasowe mogą być tworzone w tym samym czasie, na jeden plan ochrony.

Jeśli agent wykonuje kilka planów naraz, wzrasta liczba maszyn, których kopie zapasowe mogą być tworzone w tym samym czasie. Może to pogorszyć wydajność tworzenia kopii zapasowych i spowodować przeciążenie zarówno hosta, jak i magazynu maszyn wirtualnych. Takich problemów można uniknąć dzięki skonfigurowaniu ograniczenia na poziomie agenta.

Aby ograniczyć liczbę jednoczesnych operacji tworzenia kopii zapasowych na poziomie agenta

Agent dla VMware (Windows)

1. Na komputerze z agentem utwórz nowy dokument tekstowy i otwórz go w edytorze tekstów.
2. Skopiuj i wklej do pliku poniższe wiersze.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Zastąp `00000001` wartością szesnastkową limitu, który chcesz ustawić.
   Na przykład `00000001` oznacza 1, a `0000000A` oznacza 10.
4. Zapisz dokument pod nazwą **limit.reg**.
5. Uruchom plik jako administrator.
6. Potwierdź, że chcesz edytować rejestr systemu Windows.
7. Uruchom ponownie agenta.
   a. W menu **Start** kliknij **Uruchom**.
   b. Wpisz **cmd** i kliknij **OK**.
   c. W wierszu polecenia uruchom następujące polecenia:

```
net stop mms
net start mms
```

Agent dla Hyper-V

© Acronis International GmbH, 2003-2024

1. Na komputerze z agentem utwórz nowy dokument tekstowy i otwórz go w edytorze tekstów.
2. Skopiuj i wklej do pliku poniższe wiersze.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Zastąp `00000001` wartością szesnastkową limitu, który chcesz ustawić.
   Na przykład `00000001` oznacza 1, a `0000000A` oznacza 10.
4. Zapisz dokument pod nazwą **limit.reg**.
5. Uruchom plik jako administrator.
6. Potwierdź, że chcesz edytować rejestr systemu Windows.
7. Uruchom ponownie agenta.
   a. W menu **Start** kliknij **Uruchom**.
   b. Wpisz **cmd** i kliknij **OK**.
   c. W wierszu polecenia uruchom następujące polecenia:

```
net stop mms
net start mms
```

Urządzenia wirtualne

Ta procedura dotyczy agenta dla VMware (urządzenie wirtualne), agenta dla Scale Computing, agenta dla Virtuozzo Hybrid Infrastructure i agenta dla oVirt.

1. W konsoli urządzenia wirtualnego naciśnij klawisze CTRL+SHIFT+F2, aby otworzyć interfejs wiersza polecenia.
2. Otwórz plik `/etc/Acronis/MMS.config` w edytorze tekstów.
3. Odszukaj następującą sekcję:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Zastąp `10` pożądaną maksymalną liczbą jednoczesnych operacji tworzenia kopii zapasowych.
5. Zapisz plik.
6. Uruchom agenta ponownie za pomocą polecenia `reboot`.

Migracja komputera

Migracji komputera można dokonać przez odzyskanie jego kopii zapasowej na innym komputerze niż komputer pierwotny.

W poniższej tabeli zestawiono dostępne opcje migracji.

© Acronis International GmbH, 2003-2024

Typ komputera w kopii zapasowej	Dostępne lokalizacje docelowe odzyskiwania							
	Komputer fizyczny	Maszyna wirtualna ESXi	Maszyna wirtualna Hyper-V	Virtuozzo		Maszyna wirtualna Virtuozzo Hybrid Infrastructure	Maszyna wirtualna Scale Computing HC3	Maszyna wirtualna RHV/oVirt
				Maszyna wirtualna	Kontener			
Komputer fizyczny	+	+	+	-	-	+	+*	+
Maszyna wirtualna VMware ESXi	+	+	+	-	-	+	+*	+
Maszyna wirtualna Hyper-V	+	+	+	-	-	+	+*	+
Maszyna wirtualna Virtuozzo	+	+	+	+	-	+	+*	+
Kontener Virtuozzo	-	-	-	-	+	-	-	-
Maszyna wirtualna Virtuozzo Hybrid Infrastructure	+	+	+	-	-	+	+*	+
Maszyna wirtualna Scale Computing HC3	+	+	+	-	-	+	+	+
Maszyna wirtualna Red Hat Virtualization / oVirt	+	+	+	-	-	+	+*	+

© Acronis International GmbH, 2003-2024

* Jeśli na komputerze źródłowym jest włączona funkcja Secure Boot, odzyskana maszyna wirtualna nie będzie mogła zostać uruchomiona, chyba że po odzyskaniu wyłączysz funkcję Secure Boot w konsoli tej maszyny wirtualnej.

Uwaga
Nie można odzyskiwać maszyn wirtualnych macOS na hosty Hyper-V, ponieważ funkcja Hyper-V nie obsługuje systemu macOS. Maszyny wirtualne macOS można odzyskiwać na host VMware zainstalowany na sprzęcie Mac.

Dodatkowe informacje na temat wykonywania operacji migracji można znaleźć w następujących tematach:

- W przypadku migracji z komputera fizycznego na maszynę wirtualną (P2V) zobacz sekcję "Komputer fizyczny na maszynę wirtualną" (s. 538).
- W przypadku migracji z maszyny wirtualnej na maszynę wirtualną (V2V) zobacz sekcję "Odzyskiwanie maszyny wirtualnejIstnieje możliwość odzyskiwania maszyn wirtualnych z ich kopii zapasowych.W przypadku dzierżawców w trybie zgodności nie można odzyskiwać kopii zapasowych w konsoli Cyber Protect. Więcej informacji na temat odzyskiwania takich kopii zapasowych można znaleźć w sekcji "Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności" (s. 1).Wymagania wstępnePodczas odzyskiwania maszyna wirtualna nie może działać. Domyślnie oprogramowanie zatrzyma maszynę bez wyświetlenia monitu. Po zakończeniu odzyskiwania trzeba będzie ręcznie uruchomić maszynę. To domyślne zachowanie można zmienić za pomocą opcji odzyskiwania służącej do zarządzania zasilaniem maszyn wirtualnych (kliknij Opcje odzyskiwania > Zarządzanie zasilaniem maszyn wirtualnych).ProceduraWykonaj jedną z następujących czynności:Wybierz komputer uwzględniony w kopii zapasowej, kliknij Odzyskaj, a następnie wybierz punkt odzyskiwania.Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.Kliknij Odzyskaj > Cały komputer.Jeśli chcesz odzyskać na komputer fizyczny, wybierz Komputer fizyczny w polu Odzyskaj do. W przeciwnym razie pomiń ten krok.Odzyskanie na komputer fizyczny jest możliwe pod warunkiem, że konfiguracja dysków komputera docelowego jest dokładnie taka sama jak konfiguracja dysków w kopii zapasowej.W takim przypadku przejdź do kroku 4 w sekcji „Komputer fizyczny”. W przeciwnym razie zalecamy przeprowadzenie migracji maszyny wirtualnej na komputer fizyczny (V2P) przy użyciu nośnika startowego.[Opcjonalnie] Domyślnie program automatycznie wybierze pierwotny komputer jako komputer docelowy. Aby odzyskać na inną maszynę wirtualną, kliknij Komputer docelowy, a następnie wykonaj poniższe czynności:Wybierz hiperwizor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 lub oVirt).Do środowiska Virtuozzo można odzyskać tylko maszyny wirtualne Virtuozzo. Więcej informacji na temat migracji maszyny wirtualnej na maszynę wirtualną (V2V) można znaleźć w sekcji „Migracja komputera”.Określ, czy chcesz odzyskać na nową, czy na już istniejącą maszyną wirtualną.Wybierz host i określ nazwę nowej maszyny lub wybierz istniejącą maszynę docelową.Kliknij OK.Skonfiguruj dodatkowe potrzebne opcje odzyskiwania.[Możliwość niedostępna w przypadku środowisk Virtuozzo Hybrid Infrastructure i Scale Computing HC3] Aby wybrać magazyn danych dla maszyny wirtualnej, kliknij pozycję Magazyn danych w przypadku środowiska ESXi, Ścieżka w przypadku środowiska Hyper-V lub Virtuozzo lub Domena magazynu w przypadku środowiska Red Hat Virtualization (oVirt), a

 © Acronis International GmbH, 2003-2024

następnie wybierz magazyn danych (pamięć masową) dla maszyny wirtualnej.Aby wyświetlić magazyn danych (pamięć masową), interfejs i tryb alokowania dla każdego dysku wirtualnego, kliknij Mapowanie dysków. Możesz te ustawienia zmienić, chyba że odzyskujesz kontener Virtuozzo lub maszynę wirtualną Virtuozzo Hybrid Infrastructure.W przypadku środowiska Virtuozzo Hybrid Infrastructure możesz tylko wybrać zasady magazynowania dla dysków docelowych. W tym celu zaznacz żądany dysk docelowy, a następnie kliknij Zmień. W otwartym bloku kliknij ikonę koła zębatego, zaznacz zasady magazynowania, a następnie kliknij Gotowe.Sekcja mapowania umożliwia też wybranie poszczególnych dysków do odzyskania. [Dostępne w przypadku platform VMware ESXi, Hyper-V i Virtuozzo] Aby zmienić rozmiar pamięci, liczbę procesorów i połączenia sieciowe maszyny wirtualnej, kliknij Ustawienia maszyny wirtualnej.[W przypadku środowiska Virtuozzo Hybrid Infrastructure] Aby zmienić rozmiar pamięci i liczbę procesorów maszyny wirtualnej, wybierz Wariant.[Możliwość dostępna tylko w przypadku komputerów z systemem Windows, na których jest zainstalowany agent ochrony] Włącz przełącznik Bezpieczne odzyskiwanie, aby mieć pewność, że odzyskane dane będą wolne od złośliwego oprogramowania. Dodatkowe informacje na temat działania bezpiecznego odzyskiwania można znaleźć w sekcji "Bezpieczne odzyskiwanie" (s. 1).Kliknij Rozpocznij odzyskiwanie.W przypadku odzyskiwania na istniejącą maszynę wirtualną potwierdź, że chcesz zastąpić dyski.Na karcie Działania jest wyświetlany postęp odzyskiwania." (s. 1).

- W przypadku migracji z maszyny wirtualnej na komputer fizyczny (V2P) zobacz sekcje "Odzyskiwanie maszyny wirtualnejIstnieje możliwość odzyskiwania maszyn wirtualnych z ich kopii zapasowych.W przypadku dzierżawców w trybie zgodności nie można odzyskiwać kopii zapasowych w konsoli Cyber Protect. Więcej informacji na temat odzyskiwania takich kopii zapasowych można znaleźć w sekcji "Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności" (s. 1).Wymagania wstępnePodczas odzyskiwania maszyna wirtualna nie może działać. Domyślnie oprogramowanie zatrzyma maszynę bez wyświetlenia monitu. Po zakończeniu odzyskiwania trzeba będzie ręcznie uruchomić maszynę. To domyślne zachowanie można zmienić za pomocą opcji odzyskiwania służącej do zarządzania zasilaniem maszyn wirtualnych (kliknij Opcje odzyskiwania > Zarządzanie zasilaniem maszyn wirtualnych).ProceduraWykonaj jedną z następujących czynności:Wybierz komputer uwzględniony w kopii zapasowej, kliknij Odzyskaj, a następnie wybierz punkt odzyskiwania.Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.Kliknij Odzyskaj > Cały komputer.Jeśli chcesz odzyskać na komputer fizyczny, wybierz Komputer fizyczny w polu Odzyskaj do. W przeciwnym razie pomiń ten krok.Odzyskanie na komputer fizyczny jest możliwe pod warunkiem, że konfiguracja dysków komputera docelowego jest dokładnie taka sama jak konfiguracja dysków w kopii zapasowej.W takim przypadku przejdź do kroku 4 w sekcji „Komputer fizyczny”. W przeciwnym razie zalecamy przeprowadzenie migracji maszyny wirtualnej na komputer fizyczny (V2P) przy użyciu nośnika startowego.[Opcjonalnie] Domyślnie program automatycznie wybierze pierwotny komputer jako komputer docelowy. Aby odzyskać na inną maszynę wirtualną, kliknij Komputer docelowy, a następnie wykonaj poniższe czynności:Wybierz hiperwizor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 lub oVirt).Do środowiska Virtuozzo można odzyskać tylko maszyny wirtualne Virtuozzo. Więcej informacji na temat migracji maszyny wirtualnej na maszynę wirtualną (V2V) można znaleźć w sekcji „Migracja komputera”.Określ, czy chcesz odzyskać na nową, czy na już istniejącą maszyną wirtualną.Wybierz host i określ nazwę

© Acronis International GmbH, 2003-2024

nowej maszyny lub wybierz istniejącą maszynę docelową.Kliknij OK.Skonfiguruj dodatkowe potrzebne opcje odzyskiwania.[Możliwość niedostępna w przypadku środowisk Virtuozzo Hybrid Infrastructure i Scale Computing HC3] Aby wybrać magazyn danych dla maszyny wirtualnej, kliknij pozycję Magazyn danych w przypadku środowiska ESXi, Ścieżka w przypadku środowiska Hyper-V lub Virtuozzo lub Domena magazynu w przypadku środowiska Red Hat Virtualization (oVirt), a następnie wybierz magazyn danych (pamięć masową) dla maszyny wirtualnej.Aby wyświetlić magazyn danych (pamięć masową), interfejs i tryb alokowania dla każdego dysku wirtualnego, kliknij Mapowanie dysków. Możesz te ustawienia zmienić, chyba że odzyskujesz kontener Virtuozzo lub maszynę wirtualną Virtuozzo Hybrid Infrastructure.W przypadku środowiska Virtuozzo Hybrid Infrastructure możesz tylko wybrać zasady magazynowania dla dysków docelowych. W tym celu zaznacz żądany dysk docelowy, a następnie kliknij Zmień. W otwartym bloku kliknij ikonę koła zębatego, zaznacz zasady magazynowania, a następnie kliknij Gotowe.Sekcja mapowania umożliwia też wybranie poszczególnych dysków do odzyskania. [Dostępne w przypadku platform VMware ESXi, Hyper-V i Virtuozzo] Aby zmienić rozmiar pamięci, liczbę procesorów i połączenia sieciowe maszyny wirtualnej, kliknij Ustawienia maszyny wirtualnej.[W przypadku środowiska Virtuozzo Hybrid Infrastructure] Aby zmienić rozmiar pamięci i liczbę procesorów maszyny wirtualnej, wybierz Wariant.[Możliwość dostępna tylko w przypadku komputerów z systemem Windows, na których jest zainstalowany agent ochrony] Włącz przełącznik Bezpieczne odzyskiwanie, aby mieć pewność, że odzyskane dane będą wolne od złośliwego oprogramowania. Dodatkowe informacje na temat działania bezpiecznego odzyskiwania można znaleźć w sekcji "Bezpieczne odzyskiwanie" (s. 1).Kliknij Rozpocznij odzyskiwanie.W przypadku odzyskiwania na istniejącą maszynę wirtualną potwierdź, że chcesz zastąpić dyski.Na karcie Działania jest wyświetlany postęp odzyskiwania." (s. 1) i "Odzyskiwanie dysków przy użyciu nośnika startowego" (s. 544).

Migracja przy użyciu nośnika startowego

Zamiast przeprowadzać migrację komputerów w konsoli Cyber Protect, można odzyskać komputer przy użyciu nośnika startowego.

Użycie nośnika startowego jest zalecane w następujących przypadkach:

- Przeprowadzana migracja nie ma zapewnionej obsługi macierzystej.
  Można na przykład użyć nośnika startowego do odzyskania komputera fizycznego lub maszyny wirtualnej innej niż Virtuozzo jako maszyny wirtualnej Virtuozzo na hoście Virtuozzo.
- Przeprowadzana jest migracja komputera z systemem Linux zawierającego woluminy logiczne (LVM).
  Należy użyć agenta dla systemu Linux lub nośnika startowego w celu utworzenia kopii zapasowej, a następnie nośnika startowego w celu odzyskania tej kopii.
- Udostępniane są sterowniki do określonego sprzętu, co jest krytyczne z perspektywy możliwości uruchamiania systemu.
  Utwórz nośnik startowy, który może korzystać z wymaganych sterowników. Aby uzyskać więcej informacji, zobacz "Generator nośnika startowego" (s. 762).

© Acronis International GmbH, 2003-2024

Maszyny wirtualne Microsoft Azure i Amazon EC2

Aby utworzyć kopię zapasową maszyny wirtualnej Microsoft Azure lub Amazon EC2, zainstaluj na niej agenta ochrony. Tworzenie kopii zapasowych i odzyskiwanie przebiega identycznie jak w przypadku komputera fizycznego. Niemniej jednak w przypadku ustawienia limitów liczby komputerów komputer jest traktowany jako maszyna wirtualna.

Różnica w porównaniu z komputerem fizycznym polega na tym, że maszyn wirtualnych Microsoft Azure i Amazon EC2 nie można uruchamiać z nośnika startowego. Jeśli zajdzie potrzeba odzyskania na nową maszynę wirtualną Microsoft Azure lub Amazon EC2, wykonaj poniższą procedurę.

Uwaga
Poniższa procedura odzyskiwania dotyczy tylko kopii zapasowych komputerów zawierających wszystkie niezbędne sterowniki do macierzystego działania na platformie Microsoft Azure (utworzone kopie zapasowe maszyny wirtualnej Azure, lokalna maszyna Hyper-V lub komputer źródłowy z systemem Windows Server 2016 lub nowszym). Jeśli chodzi o odzyskiwanie na inną platformę, zobacz ten artykuł w bazie Knowledge Base.

Aby odzyskać komputer jako maszynę wirtualną Microsoft Azure lub Amazon EC2

1. Utwórz nową maszynę wirtualną z obrazu/szablonu w środowisku Microsoft Azure lub Amazon EC2. Nowa maszyna musi mieć taką samą konfigurację dysków jak odzyskiwany komputer.
2. Zainstaluj na nowej maszynie wirtualnej agenta dla systemu Windows lub agenta dla systemu Linux.
3. Odzyskaj komputer z kopii zapasowej zgodnie z opisem zamieszczonym w sekcji „Komputer fizyczny”. Konfigurując odzyskiwanie, wybierz nową maszynę jako komputer docelowy.

Tworzenie nośników startowych do odzyskiwania systemów operacyjnych

Nośnik startowy to dysk CD lub DVD, dysk flash USB lub inny nośnik wymienny, który umożliwia uruchomienie agenta ochrony w środowisku opartym na systemie Linux lub w środowisku preinstalacyjnym systemu Windows (WinPE)/środowisku odzyskiwania systemu Windows (WinRE) bez udziału systemu operacyjnego. Głównym zastosowaniem nośnika startowego jest odzyskiwanie systemu operacyjnego, którego nie można uruchomić.

Uwaga
Nośnik startowy nie obsługuje dysków hybrydowych.

Niestandardowy czy gotowy nośnik startowy?

Za pomocą narzędzia Bootable Media Builder można utworzyć niestandardowy nośnik startowy — oparty na systemie Linux bądź środowisku WinPE — na potrzeby komputerów z systemem Windows, Linux lub macOS. Bez względu na to, czy niestandardowy nośnik startowy jest oparty na

© Acronis International GmbH, 2003-2024

systemie Linux, czy na środowisku WinPE/WinRE, można skonfigurować ustawienia dodatkowe, takie jak automatyczna rejestracja, ustawienia sieciowe lub ustawienia serwera proxy. W przypadku niestandardowego nośnika startowego opartego na środowisku WinPE/WinRE można też zastosować dodatkowe sterowniki.

Istnieje również możliwość pobrania gotowego nośnika startowego (wyłącznie opartego na systemie Linux). Gotowego nośnika startowego można używać tylko do operacji odzyskiwania i uzyskiwania dostępu do funkcji Universal Restore.

Nośnik startowy oparty na systemie Linux czy na środowisku WinPE/WinRE?

opartym na systemie Linux

Nośnik startowy oparty na systemie Linux zawiera agenta ochrony opartego na jądrze systemu Linux. Agent może uruchamiać dowolny sprzęt klasy PC (w tym komputery bez systemu operacyjnego i komputery z uszkodzonymi lub nieobsługiwanymi systemami plików) oraz wykonywać na nim operacje.

Oparty na środowisku WinPE/WinRE

Nośnik startowy oparty na środowisku WinPE zawiera minimalną wersję systemu Windows nazywaną środowiskiem preinstalacyjnym systemu Windows (WinPE) oraz wtyczkę programu Cyber Protection do środowiska WinPE, czyli modyfikację agenta ochrony, która może działać w środowisku preinstalacyjnym. Nośnik startowy oparty na środowisku WinRE korzysta ze środowiska odzyskiwania systemu Windows i nie wymaga instalacji dodatkowych pakietów systemu Windows.

Środowisko WinPE jest najwygodniejszym rozwiązaniem startowym w dużych środowiskach wyposażonych w różnorodny sprzęt.

Zalety:

- Korzystanie z programu Cyber Protection w środowisku preinstalacyjnym systemu Windows zapewnia więcej funkcji niż korzystanie z nośnika startowego opartego na systemie Linux. Po uruchomieniu sprzętu klasy PC w środowisku WinPE można używać nie tylko agenta ochrony, ale i poleceń oraz skryptów środowiska PE, a także innych wtyczek dodanych do tego środowiska.
- Nośnik startowy oparty na środowisku PE pozwala przezwyciężyć niektóre problemy z nośnikiem startowym związane z systemem Linux, takie jak obsługa tylko niektórych kontrolerów RAID lub niektórych poziomów macierzy RAID. Nośniki oparte na środowisku WinPE 2.x lub nowszym umożliwiają dynamiczne ładowanie potrzebnych sterowników urządzeń.

Ograniczenia:

- Nośniki startowe oparte na środowisku WinPE w wersji starszej niż 4.0 nie umożliwiają uruchamiania komputerów wykorzystujących technologię Unified Extensible Firmware Interface (UEFI).

© Acronis International GmbH, 2003-2024

Tworzenie fizycznego nośnika startowego

Zdecydowanie zaleca się utworzenie i przetestowanie nośnika startowego zaraz po rozpoczęciu korzystania z kopii zapasowych na poziomie dysku. Warto też ponownie utworzyć nośnik po każdej ważnej aktualizacji agenta ochrony.

Jeden nośnik może służyć do odzyskania systemu Windows lub systemu Linux. Aby odzyskać system macOS, należy utworzyć osobny nośnik na komputerze z systemem macOS.

Aby utworzyć fizyczny nośnik startowy w systemie Windows lub Linux

1. Utwórz niestandardowy plik ISO nośnika startowego lub pobierz gotowy plik ISO.

   Aby utworzyć niestandardowy plik ISO, skorzystaj z narzędzia "Generator nośnika startowego" (s. 762).

   Aby pobrać gotowy plik ISO, w konsoli Cyber Protect wybierz komputer i kliknij **Odzyskaj** > **Więcej metod odzyskiwania** > **Pobierz obraz ISO**.
2. [Opcjonalnie] W konsoli Cyber Protect wygeneruj token rejestracji. Token rejestracji zostanie wyświetlony automatycznie w przypadku pobierania gotowego pliku ISO.

   Token ten umożliwia nośnikowi startowemu uzyskanie dostępu do chmury bez wyświetlania monitu o wprowadzenie nazwy logowania i hasła.
3. Utwórz fizyczny nośnik startowy na jeden z następujących sposobów:
   - Nagraj plik ISO na dysku CD/DVD.
   - Utwórz startowy dysk flash USB przy użyciu pliku ISO i jednego z bezpłatnych narzędzi dostępnych online.

     Użyj narzędzia `ISO to USB` lub `RUFUS`, jeśli chcesz uruchomić komputer z technologią UEFI, albo narzędzia `Win32DiskImager` w przypadku komputera z systemem BIOS. W systemie Linux warto skorzystać z narzędzia `dd`.

   W przypadku maszyn wirtualnych możesz podłączyć plik ISO jako dysk CD/DVD do maszyny, którą chcesz odzyskać.

Aby utworzyć fizyczny nośnik startowy w systemie macOS

1. Na komputerze z zainstalowanym agentem dla systemu Mac kliknij **Aplikacje** > **Generator nośnika ratunkowego**.
2. Oprogramowanie wyświetli podłączone nośniki wymienne. Wybierz ten, który ma być nośnikiem startowym.

   Ostrzeżenie!
   Wszystkie dane zapisane na dysku zostaną skasowane.

3. Kliknij **Utwórz**.
4. Poczekaj, aż oprogramowanie utworzy nośnik startowy.

© Acronis International GmbH, 2003-2024

Generator nośnika startowego

Generator nośnika startowego to specjalne narzędzie do tworzenia nośnika startowego. Jest on instalowany jako komponent opcjonalny na komputerze, na którym jest instalowany agent ochrony.

Dlaczego warto korzystać z narzędzia Bootable Media Builder?

Gotowy nośnik startowy, który jest dostępny do pobrania w konsoli Cyber Protect, jest oparty na jądrze systemu Linux. W odróżnieniu od środowiska Windows PE takie jądro nie umożliwia wprowadzania do systemu niestandardowych sterowników w locie.

Narzędzie Bootable Media Builder umożliwia tworzenie niestandardowych obrazów nośnika startowego opartych na systemie Linux lub środowisku WinPE.

32- czy 64-bitowy?

Narzędzie Bootable Media Builder obsługuje tworzenie nośników startowych z komponentami zarówno 32-, jak i 64-bitowymi. W większości przypadków do uruchomienia komputera korzystającego z interfejsu Unified Extensible Firmware Interface (UEFI) będzie potrzebny nośnik 64-bitowy.

Nośnik startowy oparty na systemie Linux

Aby utworzyć nośnik startowy oparty na systemie Linux

1. Uruchom narzędzie **Bootable Media Builder**.
2. W sekcji **Typ nośnika startowego** zaznacz **Domyślny (nośnik oparty na systemie Linux)**.
3. Wybierz sposób reprezentacji woluminów i zasobów sieciowych:
   - W przypadku nośnika startowego z reprezentacją woluminów w stylu systemu Linux są one wyświetlane na przykład jako hda1 i sdb2. Nośnik próbuje zrekonstruować urządzenia MD i woluminy logiczne (LVM) przed rozpoczęciem odzyskiwania.
   - W przypadku nośnika startowego z reprezentacją woluminów w stylu systemu Windows są one wyświetlane na przykład jako C: i D:. Nośnik zapewnia dostęp do woluminów dynamicznych (LDM).
4. [Opcjonalnie] Określ parametry jądra systemu Linux. W przypadku wielu parametrów należy je rozdzielić spacjami.

   Aby na przykład mieć możliwość wyboru trybu wyświetlania agenta startowego przy każdym uruchomieniu nośnika, wpisz: **vga=ask**. Więcej informacji o dostępnych parametrach można znaleźć w sekcji "Parametry jądra" (s. 763).
5. [Opcjonalnie] Wybierz język nośnika startowego.
6. [Opcjonalnie] Wybierz tryb startowy (BIOS lub UEFI), którego system Windows użyje po zakończeniu operacji odzyskiwania.
7. Wybierz komponent do umieszczenia na nośniku: agenta startowego Cyber Protection.

© Acronis International GmbH, 2003-2024

8. [Opcjonalnie] Określ limit czasu menu startowego. Jeśli to ustawienie nie jest skonfigurowane, program ładujący poczeka, aż zdecydujesz, czy ma zostać uruchomiony system operacyjny (jeśli jest dostępny), czy komponent.
9. [Opcjonalnie] Jeśli chcesz zautomatyzować operacje agenta startowego, zaznacz pole wyboru **Użyj następującego skryptu**. Następnie wybierz jeden ze skryptów i określ parametry skryptu. Dodatkowe informacje o skryptach można znaleźć w sekcji "Skrypty na nośniku startowym" (s. 765).
10. [Opcjonalnie] Wybierz sposób rejestracji nośnika startowego w usłudze Cyber Protection podczas uruchamiania. Dodatkowe informacje na temat ustawień rejestracji można znaleźć w sekcji "Rejestrowanie nośnika startowego" (s. 775).
11. Wybierz ustawienia sieciowe kart sieciowych uruchamianego komputera lub zachowaj automatyczną konfigurację DHCP.
12. [Opcjonalnie] Jeśli w sieci jest włączony serwer proxy, określ jego nazwę hosta lub adres IP oraz port.
13. Wybierz typ pliku utworzonego nośnika startowego:
    - Obraz ISO
    - Plik ZIP
14. Określ nazwę pliku nośnika startowego.
15. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.

Parametry jądra

Możesz podać parametry jądra systemu Linux, które zostaną automatycznie zastosowane po uruchomieniu nośnika startowego. Parametry te są przeważnie używane w razie napotkania problemów podczas pracy z nośnikiem startowym. W standardowych sytuacjach pole to może pozostać puste.

Każdy z parametrów można też określić przez naciśnięcie klawisza F11 po wyświetleniu menu startowego systemu.

Parametry

Jeśli chcesz określić wiele parametrów, rozdziel je spacjami.

- **acpi=off**

  Wyłącza interfejs zaawansowanego zarządzania energią ACPI. Warto użyć tego parametru, jeśli występują problemy z określoną konfiguracją sprzętową.
- **noapic**

  Wyłącza kontroler APIC. Warto użyć tego parametru, jeśli występują problemy z określoną konfiguracją sprzętową.
- **vga=ask**

  Wyświetla monit o wybór trybu obrazu używanego przez graficzny interfejs użytkownika nośnika startowego. W przypadku braku parametru **vga** tryb obrazu jest wybierany automatycznie.

© Acronis International GmbH, 2003-2024

- **vga=** *numer_trybu*

  Określa trybu obrazu używanego przez graficzny interfejs użytkownika nośnika startowego. Numer trybu jest określany przez wartość *numer_trybu* podawaną w formacie szesnastkowym, na przykład: **vga=0x318**

  Rozdzielczość ekranu i liczba kolorów w wybranym trybie mogą być różne na różnych komputerach. Aby wybrać odpowiednią wartość **numer_trybu**, warto najpierw użyć parametru *vga=ask*.
- **quiet**

  Wyłącza wyświetlanie komunikatów startowych podczas ładowania jądra systemu Linux, a po jego załadowaniu uruchamia konsolę zarządzania.

  Parametr ten jest określany pośrednio podczas tworzenia nośnika startowego, ale można go usunąć w menu startowym systemu.

  W przypadku jego usunięcia zostaną wyświetlone wszystkie komunikaty dotyczące uruchamiania, a następnie pojawi się wiersz polecenia. Aby uruchomić z niego konsolę zarządzania, w wierszu polecenia wpisz i uruchom polecenie **/bin/product**
- **nousb**

  Wyłącza ładowanie podsystemu obsługi interfejsu USB.
- **nousb2**

  Wyłącza obsługę interfejsu USB 2.0. Urządzenia USB 1.1 będą nadal obsługiwane. Przy użyciu tego parametru można użyć w trybie USB 1.1 tych dysków USB, które nie działają w trybie USB 2.0.
- **nodma**

  Wyłącza funkcję bezpośredniego dostępu do pamięci (DMA) dla wszystkich dysków twardych IDE. Zapobiega zawieszaniu się jądra przy niektórych urządzeniach
- **nofw**

  Wyłącz obsługę interfejsu FireWire (IEEE1394).
- **nopcmcia**

  Wyłącza wykrywanie urządzeń PCMCIA.
- **nomouse**

  Wyłącza obsługę myszy.
- *nazwa_modułu* **=off**

  Wyłącza moduł określony w parametrze *nazwa_modułu*. Aby na przykład wyłączyć obsługę modułu SATA, wpisz: **sata_sis=off**.
- **pci=bios**

  Wymusza obsługę systemu BIOS interfejsu PCI zamiast bezpośredniej. Użyj tego parametru, jeśli komputer jest wyposażony w niestandardowy mostek obsługi urządzeń PCI.
- **pci=nobios**

  Wyłącza obsługę systemu BIOS interfejsu PCI. Możliwy będzie wyłącznie bezpośredni dostęp do urządzeń. Użyj tego parametru, jeśli występują problemy z uruchomieniem nośnika startowego, które mogą być spowodowane przez system BIOS.
- **pci=biosirq**

© Acronis International GmbH, 2003-2024

Uzyskuje tabelę przekierowywania przerwań za pomocą wywołań systemu BIOS interfejsu PCI. Użyj tego parametru, jeśli jądro nie może przydzielić żądań przerwań (IRQ) lub odnaleźć dodatkowych magistrali PCI na płycie głównej.

Wywołania te mogą nie działać prawidłowo na niektórych komputerach. Jednak może być to jedyny sposób uzyskania tabeli przekierowywania przerwań.

- **LAYOUTS=en-US, de-DE, fr-FR, ...**

  Umożliwia określenie układów klawiatury, które mogą być używane w graficznym interfejsie użytkownika nośnika startowego.

  W przypadku nieokreślenia tego parametru mogą być używane tylko dwa układy: Angielski (USA) oraz układ zgodny z językiem wybranym w menu startowym nośnika.

  Można wskazać dowolny z następujących układów:

  Belgijski: **be-BE**

  Czeski: **cz-CZ**

  Angielski: **en-GB**

  Angielski (USA): **en-US**

  Francuski: **fr-FR**

  Francuski (szwajcarski): **fr-CH**

  Niemiecki: **de-DE**

  Niemiecki (szwajcarski): **de-CH**

  Włoski: **it-IT**

  Polski: **pl-PL**

  Portugalski: **pt-PT**

  Portugalski (brazylijski): **pt-BR**

  Rosyjski: **ru-RU**

  Serbski (cyrylica): **sr-CR**

  Serbski (łaciński): **sr-LT**

  Hiszpański: **es-ES**

  Podczas pracy z nośnikiem startowym możesz przechodzić między dostępnymi układami przy użyciu kombinacji klawiszy CTRL + SHIFT.

Skrypty na nośniku startowym

Jeśli nośnik startowy ma wykonywać zdefiniowany wcześniej zestaw operacji, podczas jego tworzenia w narzędziu Bootable Media Builder możesz wskazać odpowiedni skrypt. Dzięki temu przy każdym uruchamianiu komputera z tego nośnika zostanie uruchomiony wskazany skrypt i nie będzie wyświetlany interfejs użytkownika.

Program pozwala wybrać jeden ze wstępnie zdefiniowanych skryptów lub utworzyć skrypt niestandardowy zgodnie z konwencjami dotyczącymi skryptów.

Wstępnie zdefiniowane skrypty

Generator nośnika startowego zapewnia następujące wstępnie zdefiniowane skrypty:

© Acronis International GmbH, 2003-2024

- Odzyskiwanie z chmury (**entire_pc_cloud**)
- Odzyskiwanie z udziału sieciowego (**entire_pc_share**)

Skrypty znajdują się w następujących folderach na komputerze z zainstalowanym narzędziem Bootable Media Builder:

- W systemie Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- W systemie Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Odzyskiwanie z magazynu w chmurze

W generatorze nośnika startowego określ następujące parametry skryptu:

1. Nazwa pliku kopii zapasowej.
2. [Opcjonalnie] Hasło, którego skrypt będzie używać w celu uzyskiwania dostępu do zaszyfrowanych kopii zapasowych.

Odzyskiwanie z udziału sieciowego

W generatorze nośnika startowego określ następujące parametry skryptu:

- Ścieżka do udziału sieciowego.
- Nazwa użytkownika i hasło dla udziału sieciowego.
- Nazwa pliku kopii zapasowej. Aby znaleźć nazwę pliku kopii zapasowej:
  a. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych** > **Lokalizacje**.
  b. Wybierz udział sieciowy (kliknij opcję **Dodaj lokalizację**, jeśli udziału nie ma na liście).
  c. Wybierz kopię zapasową.
  d. Kliknij opcję **Szczegóły**. Nazwa pliku jest wyświetlana w pozycji **Nazwa pliku kopii zapasowej**.
- [Opcjonalnie] Hasło, którego skrypt będzie używać w celu uzyskiwania dostępu do zaszyfrowanych kopii zapasowych.

Skrypty niestandardowe

Ważne
Tworzenie skryptów niestandardowych wymaga znajomości języka poleceń Bash i notacji obiektu JavaScript (JSON). Jeśli nie znasz języka Bash, dobrym miejscem, aby się go nauczyć, jest http://www.tldp.org/LDP/abs/html. Specyfikacja notacji JSON jest dostępna pod adresem http://www.json.org

© Acronis International GmbH, 2003-2024

Pliki skryptu

Skrypt musi się znajdować w następujących katalogach na komputerze z zainstalowanym generatorem nośnika startowego:

- W systemie Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- W systemie Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Skrypt musi zawierać przynajmniej trzy pliki:

- **<script_file>.sh** — plik ze skryptem Bash. Podczas tworzenia skryptu używaj tylko ograniczonego zestawu poleceń powłoki, które możesz znaleźć pod adresem https://busybox.net/downloads/BusyBox.html. Ponadto można użyć następujących poleceń:
  - `acrocmd` — narzędzie wiersza polecenia do tworzenia kopii zapasowych i odzyskiwania
  - `product` — polecenie uruchamiające interfejs użytkownika nośnika startowego

  Ten i wszelkie dodatkowe pliki uwzględnione w skrypcie (na przykład za pomocą polecenia dot) muszą się znajdować w podfolderze **bin**. W skrypcie określ ścieżki dodatkowych plików w następującej postaci: **/ConfigurationFiles/bin/<plik>**.
- **autostart** — plik do uruchamiania pliku **<plik_skryptu>.sh**. Zawartość pliku musi być następująca:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<plik_skryptu>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** — plik JSON zawierający poniższe:
  - Nazwa i opis skryptu wyświetlane w generatorze nośnika startowego.
  - Nazwy zmiennych skryptu, które mają zostać skonfigurowane za pomocą generatora nośnika startowego.
  - Parametry elementów sterujących wyświetlane w generatorze nośnika startowego dla każdej zmiennej.

Struktura pliku autostart.json

Obiekt najwyższego poziomu

Para		Wymagane	Opis
Nazwa	**Typ wartości**		
`displayName`	ciąg	Tak	Nazwa skryptu wyświetlana w generatorze nośnika

© Acronis International GmbH, 2003-2024

			startowego.
`description`	ciąg	Nie	Opis skryptu wyświetlany w generatorze nośnika startowego.
`timeout`	liczba	Nie	Limit czasu (w sekundach) dla menu startowego przed uruchomieniem skryptu. Jeśli para nie jest określona, limit czasu będzie wynosił 10 sekund.
`variables`	obiekt	Nie	Wszelkie zmienne dla pliku **<plik_skryptu>.sh**, które chcesz skonfigurować za pomocą generatora nośnika startowego. Wartość powinna być zestawem następujących par: identyfikator ciągu zmiennej i obiekt zmiennej (patrz tabela poniżej).

Obiekt zmiennej

Para		Wymagane	Opis
Nazwa	**Typ wartości**		
`displayName`	ciąg	Tak	Nazwa zmiennej używana w pliku **<plik_skryptu>.sh**.
`type`	ciąg	Tak	Typ elementu sterującego wyświetlanego w generatorze nośnika startowego. Ten element sterujący służy do konfiguracji wartości zmiennej. Wszystkie obsługiwane typy znajdują się w poniższej tabeli.
`description`	ciąg	Tak	Etykieta elementu sterującego wyświetlana nad elementem sterującym w generatorze nośnika startowego.
`default`	ciąg, jeśli `type` to `string`, `multiString`, `password` lub `enum` liczba, jeśli `type` to `number`, `spinner` lub `checkbox`	Nie	Wartość domyślna elementu sterującego. Jeśli para nie jest określona, wartością domyślną będzie ciąg pusty lub zero w zależności od typu elementu sterującego. Wartością domyślną pola wyboru może być `0` (stan skasowany) lub `1` (stan wybrany).
`order`	liczba	Tak	Kolejność elementów sterujących w generatorze

© Acronis International GmbH, 2003-2024

	(nieujemna)		nośnika startowego. Im wyższa wartość, tym niżej element sterujący jest umieszczany względem innych elementów sterujących w pliku **autostart.json**. Wartość początkowa musi być równa `0`.
`min` (tylko dla wartości `spinner`)	liczba	Nie	Minimalna wartość pokrętła w polu pokrętła. Jeśli para nie jest określona, wartość będzie równa `0`.
`max` (tylko dla wartości `spinner`)	liczba	Nie	Maksymalna wartość pokrętła w polu pokrętła. Jeśli para nie jest określona, wartość będzie równa `100`.
`step` (tylko dla wartości `spinner`)	liczba	Nie	Wartość kroku pokrętła w polu pokrętła. Jeśli para nie jest określona, wartość będzie równa `1`.
`items` (tylko dla wartości `enum`)	tablica ciągów	Tak	Wartości dla listy rozwijanej.
`required` (dla `string`, `multiString`, `password` i `enum`)	liczba	Nie	Określa, czy wartość elementu sterującego może być pusta (`0`), czy też nie (`1`). Jeśli para nie jest określona, wartość elementu sterującego może być pusta.

Typ elementu sterującego

Nazwa	Opis
`string`	Jednowierszowe, nieograniczone pole tekstowe służące do wprowadzania lub edytowania krótkich ciągów.
`multiString`	Wielowierszowe, nieograniczone pole tekstowe służące do wprowadzania lub edytowania długich ciągów.
`password`	Jednowierszowe, nieograniczone pole tekstowe służące do bezpiecznego wprowadzania haseł.
`number`	Jednowierszowe, tylko numeryczne pole tekstowe służące do wprowadzania lub edytowania liczb.

© Acronis International GmbH, 2003-2024

spinner	Jednowierszowe, tylko numeryczne pole tekstowe służące do wprowadzania lub edytowania liczb z pokrętłem. Nazywane też polem pokrętła.
enum	Standardowa lista rozwijana ze stałym zestawem wstępnie określonych wartości.
checkbox	Pole wyboru z dwoma stanami — stanem skasowanym lub stanem wybranym.

Przykładowy plik **autostart.json** poniżej zawiera wszystkie możliwe typy elementów sterujących, których można używać do konfiguracji zmiennych dla pliku **<script_file>.sh**.

```
{
	"displayName": "Nazwa skryptu autostartu",
	"description": "To jest opis skryptu autostartu.",
	"variables": {
		"var_string": {
			"displayName": "VAR_STRING",
			"type": "string", "order": 1,
			"description": „To jest element sterujący 'string':", "default": „Witaj świecie!"
		},
		"var_multistring": {
			"displayName": "VAR_MULTISTRING",
			"type": "multiString", "order": 2,
			"description": „To jest element sterujący 'multiString':",
			"default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
		},
		"var_number": {
			"displayName": "VAR_NUMBER",
			"type": "number", "order": 3,
			"description": „To jest element sterujący 'number':", "default": 10
		},
		"var_spinner": {
			"displayName": "VAR_SPINNER",
			"type": "spinner", "order": 4,
			"description": „To jest element sterujący 'spinner':",
```


© Acronis International GmbH, 2003-2024

```
                        "min": 1, "max": 10, "step": 1, "default": 5
                },
                "var_enum": {
                        "displayName": "VAR_ENUM",
                        "type": "enum", "order": 5,
                        "description": „To jest element sterujący 'enum':",
                        "items": ["pierwszy", "drugi", "trzeci"], "default": "drugi"
                },
                "var_password": {
                        "displayName": "VAR_PASSWORD",
                        "type": "password", "order": 6,
                        "description": „To jest element sterujący 'password':", "default”:
"qwe"
                },
                "var_checkbox": {
                        "displayName": "VAR_CHECKBOX",
                        "type": "checkbox", "order": 7,
                        "description": „To jest element sterujący 'checkbox':", "default": 1
                }
        }
}
```

Nośnik startowy oparty na środowisku WinPE i WinRE

Możesz tworzyć obrazy WinRE bez dodatkowych przygotowań lub tworzyć obrazy WinPE po zainstalowaniu Zestawu zautomatyzowanej instalacji systemu Windows (AIK) bądź Zestawu do oceny i wdrażania systemu Windows (ADK).

Obrazy WinRE

Tworzenie obrazów WinRE jest obsługiwane przez następujące systemy operacyjne:

- Windows 7 (64-bitowy)
- Windows 8 (wersja 32-bitowa i 64-bitowa)
- Windows 8.1 (wersja 32-bitowa i 64-bitowa)
- Windows 10 (wersja 32-bitowa i 64-bitowa)

© Acronis International GmbH, 2003-2024

- Windows 11 (wersja 64-bitowa)
- Windows Server 2012 (wersja 64-bitowa)
- Windows Server 2016 (wersja 64-bitowa)
- Windows Server 2019 (wersja 64-bitowa)
- Windows Server 2022 (wersja 64-bitowa)

Obrazy WinPE

Po zainstalowaniu Zestawu zautomatyzowanej instalacji systemu Windows (AIK) bądź Zestawu do oceny i wdrażania systemu Windows (ADK) Generator nośnika startowego obsługuje dystrybucje środowiska WinPE oparte na następujących jądrach:

- Windows Vista (PE 2.0)
- Windows Vista z dodatkiem SP1 i Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) z uzupełnieniem dla systemu Windows 7 z dodatkiem SP1 (PE 3.1) lub bez niego
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Program Bootable Media Builder obsługuje 32- oraz 64-bitowe dystrybucje środowiska WinPE. 32-bitowa dystrybucja środowiska WinPE może działać także na sprzęcie 64-bitowym. Jednak do uruchomienia komputera korzystającego z interfejsu Unified Extensible Firmware Interface (UEFI) potrzebna jest dystrybucja 64-bitowa.

Uwaga
Do działania obrazów PE opartych na środowisku WinPE 4 lub nowszym wymagany jest przynajmniej 1 GB pamięci RAM.

Tworzenie nośnika startowego WinPE lub WinRE

Bootable Media Builder udostępnia dwie metody integracji usługi Cyber Protection ze środowiskiem WinPE i WinRE:

- Tworzenie pliku ISO od początku za pomocą wtyczki Cyber Protection.
- Dodanie wtyczki Cyber Protection Plug-in do pliku WIM na potrzeby dowolnych przyszłych celów (ręcznego wygenerowania obrazu ISO, dodawania innych narzędzi do obrazu itd.).

Aby utworzyć nośnik startowy WinPE lub WinRE

1. Na komputerze z zainstalowanym agentem ochrony uruchom narzędzie Bootable Media Builder.
2. W sekcji **Typ nośnika startowego** zaznacz **Windows PE** lub **Windows PE (64-bitowe)**. Nośnik 64-bitowy jest potrzebny do uruchomienia komputera korzystającego z interfejsu Unified

© Acronis International GmbH, 2003-2024

Extensible Firmware Interface (UEFI).

3. Wybierz podtyp nośnika startowego: **WinRE** lub **WinPE**.

   Utworzenie nośnika startowego WinRE nie wymaga zainstalowania żadnych dodatkowych pakietów.

   Aby utworzyć nośnik oparty na 64-bitowym środowisku WinPE, trzeba pobrać Zestaw zautomatyzowanej instalacji systemu Windows (AIK) lub Zestaw do oceny i wdrażania systemu Windows (ADK). Aby utworzyć nośnik oparty na 32-bitowym środowisku WinPE, oprócz pobrania zestawu AIK lub ADK wykonaj również następujące czynności:

   a. Kliknij **Pobierz wtyczkę dla środowiska WinPE (32-bitową)**.

   b. Zapisz wtyczkę w folderze **%PROGRAM_ FILES%\BackupClient\BootableComponents\WinPE32**.

4. [Opcjonalnie] Wybierz język nośnika startowego.
5. [Opcjonalnie] Wybierz tryb startowy (BIOS lub UEFI), którego system Windows użyje po zakończeniu operacji odzyskiwania.
6. Wybierz ustawienia sieciowe kart sieciowych uruchamianego komputera lub zachowaj automatyczną konfigurację DHCP.
7. [Opcjonalnie] Wybierz sposób rejestracji nośnika startowego w usłudze Cyber Protection podczas uruchamiania. Dodatkowe informacje na temat ustawień rejestracji można znaleźć w sekcji "Rejestrowanie nośnika startowego" (s. 775).
8. [Opcjonalnie] Określ sterowniki systemu Windows, które chcesz dodać do nośnika startowego.

   Po uruchomieniu komputera w środowisku Windows PE lub Windows RE sterowniki te ułatwią uzyskanie dostępu do urządzenia, na którym znajduje się kopia zapasowa. Dodaj sterowniki 32-bitowe, jeśli jest używana 32-bitowa dystrybucja środowiska WinPE lub WinRE, albo sterowniki 64-bitowe w przypadku 64-bitowej dystrybucji środowiska WinPE lub WinRE.

   Aby dodać sterowniki:

   - Kliknij **Dodaj** i określ ścieżkę do niezbędnego pliku .inf dla odpowiadającego mu kontrolera SCSI, RAID lub SATA, karty sieciowej, napędu taśmowego albo innego urządzenia.
   - Powtórz tę procedurę w odniesieniu do każdego sterownika, który chcesz dołączyć do wynikowego nośnika środowiska WinPE lub WinRE.

9. Wybierz typ pliku utworzonego nośnika startowego:
   - Obraz ISO
   - Obraz WIM
10. Określ pełną ścieżkę wynikowego pliku obrazu, włącznie z nazwą pliku.
11. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.

Aby utworzyć obraz środowiska PE (plik ISO) z wynikowego pliku WIM

- Zastąp domyślny plik boot.wim w folderze środowiska Windows PE nowo utworzonym plikiem WIM. W powyższym przykładzie wpisz:

```
Skopiuj plik c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```


© Acronis International GmbH, 2003-2024

- Użyj narzędzia **Oscdimg**. W powyższym przykładzie wpisz:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Ostrzeżenie!
Nie kopiuj i nie wklejaj tego przykładu. Wpisz polecenie ręcznie, ponieważ w przeciwnym razie jego wykonanie się nie powiedzie.

Przygotowanie: Środowisko WinPE 2.x lub 3.x

Aby można było tworzyć lub modyfikować obrazy środowiska PE 2.x lub 3.x, zainstaluj Generator nośnika startowego i Zestaw zautomatyzowanej instalacji systemu Windows (Automated Installation Kit, AIK) na tym samym komputerze.

Aby przygotować komputer

1. Pobierz plik obrazu AIK z witryny internetowej firmy Microsoft w następujący sposób:
   - W przypadku systemu Windows Vista (PE 2.0): https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - W przypadku systemu Windows Vista SP1 lub Windows Server 2008 (PE 2.1): https://www.microsoft.com/en-us/download/details.aspx?id=9085
   - W przypadku systemu Windows 7 (PE 3.0): https://www.microsoft.com/en-gb/download/details.aspx?id=5753

     W przypadku systemu Windows 7 SP1 (PE 3.1) potrzebny jest także dodatek AIK dostępny pod adresem https://www.microsoft.com/en-us/download/details.aspx?id=5188
2. Nagraj plik obrazu na dysk DVD lub dysk flash USB.
3. Zainstaluj następujące elementy z pliku obrazu:
   - Microsoft .NET Framework (NETFXx86 lub NETFXx64, w zależności od sprzętu)
   - MSXML (analizator składni XML firmy Microsoft)
   - Windows AIK
4. Zainstaluj Generator nośnika startowego na tym samym komputerze.

Przygotowanie: środowisko WinPE 4.0 lub nowsze

Aby można było tworzyć lub modyfikować obrazy środowiska PE w wersji 4 lub nowszej, zainstaluj Generator nośnika startowego i Zestaw do oceny i wdrażania systemu Windows (Assessment and Deployment Kit, ADK) na tym samym komputerze.

Aby przygotować komputer

1. Pobierz program instalacyjny ADK z witryny internetowej firmy Microsoft .

   Obsługiwane są następujące wersje systemu Windows:
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)

© Acronis International GmbH, 2003-2024

- Windows 8.1 (PE 5.0)
- Windows 8 (PE 4.0)

2. Zainstaluj Zestaw do oceny i wdrażania.
3. Zainstaluj Generator nośnika startowego.

Rejestrowanie nośnika startowego

Zarejestrowanie nośnika startowego w usłudze Cyber Protection umożliwia uzyskiwanie dostępu do kopii zapasowych w chmurze. Podczas tworzenia nośnika startowego można wstępnie skonfigurować rejestrację. Jeśli rejestracja nie zostanie wstępnie skonfigurowana, można zarejestrować nośnik po uruchomieniu komputera za jego pomocą.

Aby wstępnie skonfigurować rejestrację w usłudze Cyber Protection

1. W narzędziu Bootable Media Builder przejdź do sekcji **Rejestracja nośnika startowego**.
2. W obszarze **Adres URL usługi** podaj adres usługi Cyber Protection.
3. [Opcjonalnie] W polu **Nazwa wyświetlana** określ nazwę uruchamianego komputera.
4. Aby ustawić automatyczną rejestrację w usłudze Cyber Protection, zaznacz pole wyboru **Zarejestruj nośnik startowy automatycznie** i wybierz poziom rejestracji automatycznej:
   - **Podczas uruchamiania komputera zapytaj o token rejestracji**
     Token trzeba wprowadzać przy każdym uruchamianiu komputera z danego nośnika startowego.
   - **Użyj następującego tokenu**
     Komputer będzie rejestrowany automatycznie przy każdym uruchamianiu z danego nośnika startowego.

Aby zarejestrować nośnik startowy po uruchomieniu komputera za jego pomocą

1. Uruchom komputer za pomocą nośnika startowego.
2. W oknie uruchamiania kliknij **Zarejestruj nośnik**.
3. W polu **Serwer** podaj adres usługi Cyber Protection.
4. W polu **Token rejestracji** wprowadź token rejestracji.
5. Kliknij **Zarejestruj**.

Ustawienia sieciowe

Tworząc nośnik startowy, możesz wstępnie skonfigurować połączenia sieciowe, które będą używane przez agenta startowego. Można wstępnie skonfigurować następujące parametry:

- Adres IP
- Maska podsieci
- brama,

© Acronis International GmbH, 2003-2024

- Serwer DNS
- Serwer WINS

Po uruchomieniu agenta startowego na komputerze konfiguracja jest stosowana do karty sieciowej tego komputera. Jeśli ustawienia nie zostały wstępnie skonfigurowane, agent używa automatycznej konfiguracji DHCP.

Po uruchomieniu agenta startowego na komputerze ustawienia sieciowe można też skonfigurować ręcznie.

Wstępne konfigurowanie wielu połączeń sieciowych

Można wstępnie skonfigurować ustawienia TCP/IP dla nawet dziesięciu kart sieciowych. Aby mieć pewność, że do każdej karty sieciowej zostaną przypisane właściwe ustawienia, należy utworzyć nośnik na serwerze, do którego nośnik został dostosowany. Gdy zaznaczysz istniejącą kartę sieciową w oknie kreatora, jej ustawienia zostają wybrane i zapisane na nośniku. Na nośniku jest też zapisywany adres MAC każdej dostępnej karty sieciowej.

Ustawienia te, z wyjątkiem adresu MAC, można zmienić. W razie potrzeby można też skonfigurować ustawienia nieistniejącej karty NIC.

Gdy agent startowy uruchomi się na serwerze, pobiera listę dostępnych kart sieciowych. Lista ta jest uporządkowana według gniazd zajmowanych przez karty: na początku są wymienione karty znajdujące się najbliżej procesora.

Agent startowy przypisuje odpowiednie ustawienia każdej znanej karcie sieciowej i rozpoznaje poszczególne karty na podstawie ich adresów MAC. Po skonfigurowaniu kart sieciowych o znanych adresach MAC do pozostałych kart są przypisywane ustawienia określone dla kart nieistniejących, począwszy od znajdującej się najwyżej nieprzypisanej karty.

Nośnik startowy można dostosować pod kątem każdego komputera — nie tylko tego, na którym nośnik został utworzony. W tym celu należy skonfigurować karty sieciowe zgodnie z kolejnością ich gniazd w komputerze: Karta NIC1 zajmuje gniazdo znajdujące się najbliżej procesora, karta NIC2 kolejne gniazdo itd. Gdy agent startowy uruchomi się na komputerze, nie znajdzie żadnej karty sieciowej ze znanym adresem MAC, w związku z czym skonfiguruje karty w takiej samej kolejności.

Przykład

Agent startowy może używać jednej z kart sieciowych do komunikacji z konsolą zarządzania za pośrednictwem sieci produkcyjnej. Połączenie to może zostać skonfigurowane automatycznie. Duże ilości danych związanych z odzyskiwaniem można przesłać za pośrednictwem drugiej karty sieciowej, uwzględnionej w odrębnej sieci tworzenia kopii zapasowych przy użyciu statycznych ustawień TCP/IP.

© Acronis International GmbH, 2003-2024

Nawiązywanie połączenia z komputerem uruchomionym z nośnika startowego

Połączenie lokalne

Aby działać bezpośrednio na komputerze uruchomionym za pomocą nośnika startowego, w oknie startowym kliknij **Zarządzaj tym komputerem lokalnie**.

Po uruchomieniu komputera z nośnika startowego na terminalu komputera zostanie wyświetlone okno startowe z adresami IP uzyskanymi z serwera DHCP lub ustawionymi zgodnie z wcześniej skonfigurowanymi wartościami.

Konfigurowanie ustawień sieciowych

Aby zmienić ustawienia sieciowe dla bieżącej sesji, w oknie startowym kliknij **Konfiguruj sieć**. Zostanie wyświetlone okno **Ustawienia sieciowe**, które umożliwia skonfigurowanie ustawień sieciowych każdej karty sieciowej (NIC) komputera.

Zmiany wprowadzone w trakcie sesji zostaną utracone po ponownym uruchomieniu komputera.

Dodawanie sieci VLAN

W oknie **Ustawienia sieciowe** można dodawać wirtualne sieci lokalne (VLAN). Funkcja ta jest przydatna, jeśli wymagany jest dostęp do lokalizacji kopii zapasowych uwzględnionej w określonej sieci VLAN.

Sieci VLAN służą głównie do dzielenia sieci lokalnych na segmenty. Karta sieciowa (NIC) podłączona do portu *access* przełącznika ma zawsze dostęp do sieci VLAN określonej w konfiguracji portu. Karta sieciowa (NIC) podłączona do portu *trunk* przełącznika ma dostęp do sieci VLAN dozwolonych w konfiguracji portu tylko w przypadku, gdy sieci te zostały określone w ustawieniach sieciowych.

Aby umożliwić dostęp do sieci VLAN za pomocą portu trunk

1. Kliknij **Dodaj sieć VLAN**.
2. Wybierz kartę sieciową, która umożliwia dostęp do sieci lokalnej obejmującej wymaganą sieć VLAN.
3. Określ identyfikator sieci VLAN.

Po kliknięciu **OK** na liście kart sieciowych pojawi się nowa pozycja.

Jeśli konieczne jest usunięcie sieci VLAN, kliknij pozycję odpowiadającą żądanej sieci VLAN, a następnie kliknij **Usuń sieć VLAN**.

Lokalne operacje wykonywane przy użyciu nośnika startowego

Operacje wykonywane przy użyciu nośnika startowego przypominają operacje odzyskiwania wykonywane w ramach działającego systemu operacyjnego. Różnice są następujące:

© Acronis International GmbH, 2003-2024

1. W przypadku nośnika startowego z reprezentacją woluminów w stylu systemu Windows wolumin ma taką samą literę dysku jak w systemie Windows. Do woluminów, które nie mają litery dysku w systemie Windows (takich jak wolumin Zastrzeżone przez system), przypisywane są wolne litery w takiej kolejności, w jakiej woluminy występują na dysku.

   Jeśli nośnik startowy nie wykryje na komputerze systemu Windows lub wykryje więcej niż jeden system, do wszystkich woluminów (włącznie z woluminami bez liter dysku) litery są przypisywane w takiej kolejności, w jakiej te woluminy występują na dysku. Oznacza to, że litery woluminów mogą się różnić od liter w systemie Windows. Na przykład dysk D: na nośniku startowym może odpowiadać dyskowi E: w systemie Windows.

   Uwaga
   Ze względów bezpieczeństwa warto przypisać woluminom unikatowe nazwy.

2. W przypadku nośnika startowego z takimi woluminami jak w systemie Linux dyski lokalne i woluminy są wyświetlane jako niezamontowane (sda1, sda2...).
3. Zadań nie można planować. Jeśli trzeba powtórzyć operację, należy skonfigurować ją od początku.
4. Czas życia dziennika jest ograniczony do bieżącej sesji. Cały dziennik lub odfiltrowane wpisy dziennika można zapisać w pliku.

Konfigurowanie trybu wyświetlania

W przypadku uruchamiania komputera przy użyciu nośnika startowego opartego na systemie Linux tryb wyświetlania obrazu wideo jest wykrywany automatycznie na podstawie konfiguracji sprzętowej (danych technicznych monitora i karty graficznej). Jeśli tryb wideo jest wykrywany niepoprawnie, wykonaj następujące czynności:

1. W menu startowym naciśnij F11.
2. Wpisz w wierszu polecenia: **vga=ask** i kontynuuj uruchamianie.
3. Z listy obsługiwanych trybów wideo wybierz odpowiedni tryb, wpisując jego numer (na przykład **318**), a następnie naciśnij klawisz **Enter**.

Jeśli nie chcesz wykonywać tej procedury przy każdym uruchamianiu danej konfiguracji sprzętowej, ponownie utwórz nośnik startowy, wprowadzając odpowiedni numer trybu (w tym przykładzie: **vga=0x318**) w polu **Parametry jądra**.

Odzyskiwanie lokalne przy użyciu nośnika startowego

1. Uruchom komputer za pomocą nośnika startowego.
2. Kliknij **Zarządzaj tym komputerem lokalnie**.
3. Kliknij **Odzyskaj**.
4. W sekcji **Elementy do odzyskania** kliknij **Wybierz dane**.
5. Wybierz plik kopii zapasowej, z którego chcesz odzyskać dane.

© Acronis International GmbH, 2003-2024

6. W lewym dolnym okienku wybierz dyski/woluminy lub pliki/foldery, które chcesz odzyskać, a następnie kliknij **OK**.
7. Skonfiguruj reguły zastępowania.
8. Skonfiguruj wykluczenia z odzyskiwania.
9. Skonfiguruj opcje odzyskiwania.
10. Sprawdź, czy ustawienia są prawidłowe, i kliknij **OK**.

Operacje zdalne dotyczące nośnika startowego

Uwaga
Ta funkcja jest dostępna w pakiecie Zaawansowane tworzenie kopii zapasowych.

Aby nośnik startowy był widoczny w konsoli Cyber Protect, trzeba najpierw go zarejestrować zgodnie z opisem podanym w sekcji "Rejestrowanie nośnika startowego" (s. 775).

Po zarejestrowaniu nośnika w konsoli Cyber Protect będzie on widoczny na karcie **Urządzenia** > **Nośnik startowy**. Nośnik startowy zniknie z tej karty po ponad 30 dniach w trybie offline.

Nośnikiem startowym można zarządzać zdalnie w konsoli Cyber Protect. Można na przykład odzyskać dane, uruchomić ponownie komputer uruchomiony przy użyciu nośnika lub zamknąć system takiego komputera, a także wyświetlić informacje, działania i alerty dotyczące nośnika.

Ważne
Nie można zaktualizować nośnika startowego zdalnie na karcie **Ustawienia** > **Agenci** w konsoli Cyber Protect.

Aby zaktualizować nośnik startowy, należy utworzyć nowy zgodnie z opisem podanym w sekcji "Generator nośnika startowego" (s. 762). Alternatywnie można pobrać gotowy nośnik, klikając ikonę konta > **Do pobrania** > **Nośnik startowy** w konsoli Cyber Protect.

Aby zdalnie odzyskać pliki lub foldery przy użyciu nośnika startowego

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Nośnik startowy**.
1. Wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Odzyskiwanie**.
3. Wybierz lokalizację, a następnie potrzebną kopię zapasową. Należy pamiętać, że kopie zapasowe są filtrowane według lokalizacji.
4. Wybierz punkt odzyskiwania, a następnie kliknij **Odzyskaj pliki/foldery**.
5. Przejdź do odpowiedniego folderu lub użyj paska wyszukiwania, aby uzyskać listę wymaganych plików i folderów.
   Wyszukiwanie zależy od języka.

© Acronis International GmbH, 2003-2024

Można użyć jednego lub kilku symboli wieloznacznych (* i ?). Więcej informacji na temat stosowania symboli wieloznacznych można znaleźć w sekcji "Filtry plików (uwzględniające/wykluczające)" (s. 494).

6. Kliknij, aby wybrać pliki, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
7. W polu **Ścieżka** wybierz miejsce docelowe odzyskiwania.
8. [Opcjonalnie] Aby przeprowadzić zaawansowaną konfigurację odzyskiwania, kliknij **Opcje odzyskiwania**. Więcej informacji można znaleźć w sekcji "Opcje odzyskiwania" (s. 558).
9. Kliknij **Rozpocznij odzyskiwanie**.
10. Wybierz jedną z następujących opcji zastępowania plików:
    - **Zastąp istniejące pliki**
    - **Zastąp istniejący plik, jeśli jest starszy**
    - **Nie zastępuj istniejących plików**

    Określ, czy komputer ma zostać automatycznie ponownie uruchomiony.
11. Kliknij **Kontynuuj**, aby rozpocząć odzyskiwanie. Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby zdalnie odzyskać dyski, woluminy lub całe komputery przy użyciu nośnika startowego

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Odzyskiwanie**.
3. Wybierz lokalizację, a następnie potrzebną kopię zapasową. Należy pamiętać, że kopie zapasowe są filtrowane według lokalizacji.
4. Wybierz punkt odzyskiwania, a następnie kliknij **Odzyskaj** > **Cały komputer**.
   W razie potrzeby skonfiguruj komputer docelowy i mapowanie woluminów zgodnie z opisem podanym w sekcji "Odzyskiwanie komputerów fizycznychW tej sekcji opisano odzyskiwanie komputerów fizycznych przy użyciu interfejsu internetowego.Czasem lepiej użyć nośnika startowego, a nie interfejsu internetowego. Dotyczy to odzyskiwania następujących elementów:Komputer z systemem macOSKomputer z obszaru dzierżawcy w trybie zgodnościDowolny system operacyjny na komputer bez systemu operacyjnego lub komputer w trybie offlineStruktura woluminów logicznych (woluminy utworzone przez narzędzie Logical Volume Manager w systemie Linux). Nośnik umożliwia automatyczne odtworzenie struktury woluminu logicznego.Nie można odzyskać kopii zapasowych na poziomie dysku z komputerów Mac z procesorami Intel na komputery Mac z procesorami Apple Silicon i na odwrót. Można odzyskać pliki i foldery.Aby odzyskać komputer fizycznyWybierz komputer uwzględniony w kopii zapasowej.Kliknij Odzyskiwanie.Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:Jeśli lokalizacją kopii zapasowych jest chmura lub współdzielony magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij Wybierz komputer, wybierz komputer docelowy będący w trybie online i wybierz punkt odzyskiwania.Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.Odzyskaj

© Acronis International GmbH, 2003-2024

komputer zgodnie z instrukcjami podanymi w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego”.Kliknij Odzyskaj > Cały komputer.Program automatycznie zamapuje dyski z kopii zapasowej na dyski komputera docelowego.Aby odzyskać na inny komputer fizyczny, kliknij Komputer docelowy i wybierz komputer docelowy będący w trybie online.Jeśli mapowanie dysku się nie powiedzie lub będzie niezgodne z oczekiwaniami, kliknij Mapowanie woluminów, aby zamapować dyski ręcznie.Sekcja mapowania umożliwia też wybranie poszczególnych dysków lub woluminów do odzyskania. Możesz przełączać się między dyskami i woluminami do odzyskania przy użyciu linku Przełącz na... w prawym górnym rogu.[Możliwość dostępna tylko w przypadku komputerów z systemem Windows, na których jest zainstalowany agent ochrony] Włącz przełącznik Bezpieczne odzyskiwanie, aby mieć pewność, że odzyskane dane będą wolne od złośliwego oprogramowania. Dodatkowe informacje na temat działania bezpiecznego odzyskiwania można znaleźć w sekcji "Bezpieczne odzyskiwanie" (s. 1).Kliknij Rozpocznij odzyskiwanie.Potwierdź, że chcesz zastąpić dyski ich wersjami z kopii zapasowej. Określ, czy komputer ma zostać automatycznie ponownie uruchomiony.Na karcie Działania jest wyświetlany postęp odzyskiwania." (s. 1).

5. Aby przeprowadzić zaawansowaną konfigurację odzyskiwania, kliknij **Opcje odzyskiwania**. Więcej informacji można znaleźć w sekcji "Opcje odzyskiwania" (s. 558).
6. Kliknij **Rozpocznij odzyskiwanie**.
7. Potwierdź, że chcesz zastąpić dyski ich wersjami z kopii zapasowej. Określ, czy komputer ma zostać automatycznie ponownie uruchomiony.
8. Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby zdalnie uruchomić ponownie komputer uruchomiony przy użyciu nośnika

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Uruchom ponownie**.
3. Potwierdź, że chcesz uruchomić ponownie komputer uruchomiony przy użyciu nośnika.

Aby zdalnie zamknąć system komputera uruchomionego przy użyciu nośnika

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Zamknij system**.
3. Potwierdź, że chcesz zamknąć system komputera uruchomionego przy użyciu nośnika.

Aby wyświetlić informacje o nośniku startowym

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Szczegóły**, **Działania** lub **Alerty**, aby wyświetlić odpowiednie informacje.

Aby zdalnie usunąć nośnik startowy

© Acronis International GmbH, 2003-2024

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Usuń**, aby usunąć nośnik startowy z konsoli Cyber Protect.
3. Potwierdź, że chcesz usunąć nośnik startowy.

Startup Recovery Manager

Startup Recovery Manager to komponent startowy znajdujący się na dysku twardym. Za pomocą komponentu Startup Recovery Manager można uruchomić ratunkowe narzędzie startowe bez korzystania z osobnego nośnika startowego.

W przypadku niepowodzenia operacji uruchom ponownie komputer, poczekaj na wyświetlenie monitu **Naciśnij klawisz F11, aby uruchomić AcronisStartup Recovery Manager**, a następnie naciśnij klawisz F11 lub wybierz Startup Recovery Manager z menu startowego (jeśli korzystasz z programu ładującego GRUB). Zostanie uruchomione narzędzie Startup Recovery Manager i będzie można przeprowadzić odzyskiwanie.

Startup Recovery Manager jest obsługiwany w przypadku komputerów z systemem Windows i Linux.

Ważne
Aktywacja narzędzia Startup Recovery Manager na komputerze z zaszyfrowanym woluminem systemowym wymaga co najmniej jednego niezaszyfrowanego woluminu na tym samym komputerze.

Wymagania dotyczące miejsca na dysku

Startup Recovery Manager wymaga miejsca na dysku na pliki tymczasowe. Wymagania różnią się w zależności od komputera, na którym jest aktywowane narzędzie Startup Recovery Manager.

W poniższej tabeli zestawiono dostępne opcje.

Tryb startowy	Komputer bez partycji Secure Zone		Komputer z partycją Secure Zone
	Z niezaszyfrowanym woluminem systemowym	**Z zaszyfrowanym woluminem systemowym**	**Z zaszyfrowanym lub niezaszyfrowanym woluminem systemowym**
BIOS	200 MB na woluminie systemowym	400 MB na woluminie niezaszyfrowanym	400 MB na partycji Secure Zone
UEFI	200 MB na partycji systemowej EFI (ESP)	Jedna z następujących możliwości: • 400 MB na partycji systemowej EFI (ESP)	400 MB na partycji Secure Zone

© Acronis International GmbH, 2003-2024

Tryb startowy	Komputer bez partycji Secure Zone		Komputer z partycją Secure Zone
	Z niezaszyfrowanym woluminem systemowym	Z zaszyfrowanym woluminem systemowym	Z zaszyfrowanym lub niezaszyfrowanym woluminem systemowym
		• 200 MB na partycji systemowej EFI (ESP) i 200 MB na partycji niezaszyfrowanej dostępnej podczas procesu uruchamiania	

Uwaga
Odzyskiwanie po ponownym uruchomieniu wymaga dodatkowego miejsca na dysku. Aby sprawdzić zapotrzebowanie na dodatkowe miejsce, zobacz sekcję "Wymagania dotyczące miejsca na dysku" (s. 543).

Ograniczenia

- [Nie dotyczy programu ładującego GRUB zainstalowanego w głównym rekordzie startowym] Aktywacja narzędzia Startup Recovery Manager powoduje zastąpienie głównego rekordu startowego (master boot record, MBR) własnym kodem startowym. W wyniku tego po aktywacji może być konieczne ponowne aktywowanie startowych programów ładujących innych firm.
- [Nie dotyczy programu ładującego GRUB] Przed aktywacją narzędzia Startup Recovery Manager w systemie Linux warto zainstalować startowy program ładujący w rekordzie startowym partycji głównej lub w rekordzie startowym partycji /boot, a nie w głównym rekordzie startowym. Jeśli wybierzesz inne rozwiązanie, po aktywacji ręcznie skonfiguruj startowy program ładujący.

Aktywowanie programu Startup Recovery Manager

Aby włączyć monit **Naciśnij klawisz F11, aby uruchomić AcronisStartup Recovery Manager** wyświetlany w czasie uruchamiania (lub dodać pozycję **Startup Recovery Manager** do menu programu ładującego GRUB), musisz aktywować narzędzie Startup Recovery Manager.

Uwaga
Operacje tworzenia kopii zapasowych, które powodują tworzenie kopii zapasowych obsługujących odzyskiwanie jednym kliknięciem, się nie powiodą, jeśli nie jest aktywowane narzędzie Startup Recovery Manager.

Aby aktywować narzędzie Startup Recovery Manager

Na komputerze z agentem

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect wybierz komputer, na którym chcesz aktywować narzędzie Startup Recovery Manager.
2. Kliknij opcję **Szczegóły**.
3. Włącz przełącznik **Startup Recovery Manager**.

Na komputerze bez agenta

1. Uruchom komputer przy użyciu nośnika startowego.
2. W graficznym interfejsie nośnika startowego kliknij **Narzędzia** > **AktywujStartup Recovery Manager**.
3. Wybierz **Aktywuj**.
4. Kliknij **OK**.
5. Na karcie **Szczegóły** sprawdź w wierszu **Wynik**, czy aktywacja się powiodła.
6. Kliknij **Zamknij**.

Dezaktywowanie programu Startup Recovery Manager

Dezaktywacja powoduje wyłączenie monitu **Naciśnij klawisz F11, aby uruchomić AcronisStartup Recovery Manager** wyświetlanego w czasie uruchamiania (lub usunięcie pozycji **Startup Recovery Manager** z menu programu ładującego GRUB).

Jeśli narzędzie Startup Recovery Manager nie jest aktywowane, nadal możesz odzyskać komputer, którego nie można uruchomić — za pomocą osobnego nośnika startowego.

Uwaga
Operacje tworzenia kopii zapasowych, które powodują tworzenie kopii zapasowych obsługujących odzyskiwanie jednym kliknięciem, się nie powiodą, jeśli nie jest aktywowane narzędzie Startup Recovery Manager.

Aby dezaktywować narzędzie Startup Recovery Manager

Na komputerze z agentem

1. W konsoli Cyber Protect wybierz komputer, na którym chcesz dezaktywować narzędzie Startup Recovery Manager.
2. Kliknij opcję **Szczegóły**.
3. Wyłącz przełącznik **Startup Recovery Manager**.

Na komputerze bez agenta

1. Uruchom komputer przy użyciu nośnika startowego.
2. W graficznym interfejsie nośnika startowego kliknij **Narzędzia** > **Dezaktywuj Startup Recovery Manager**.
3. Wybierz **Dezaktywuj**.
4. Kliknij **OK**.

© Acronis International GmbH, 2003-2024

5. Na karcie **Szczegóły** sprawdź w wierszu **Wynik**, czy dezaktywacja się powiodła.
6. Kliknij **Zamknij**.

© Acronis International GmbH, 2003-2024

Wdrażanie funkcji odzyskiwania po awarii

Uwaga
Ta funkcja nie obsługuje lokalizacji kopii zapasowych na platformie Microsoft Azure.

Cyber Disaster Recovery Cloud — informacje

Cyber Disaster Recovery Cloud (DR) — wchodzące w skład platformy Cyber Protection rozwiązanie DRaaS (odzyskiwanie po awarii jako usługa). Cyber Disaster Recovery Cloud to szybkie i stabilne rozwiązanie, które pozwala uruchamiać dokładne kopie swoich komputerów w lokalizacji w chmurze i przenosić obciążenia z uszkodzonych oryginalnych komputerów na serwery odzyskiwania w chmurze w razie szkód spowodowanych przez człowieka lub katastrofę naturalną.

Środowisko odzyskiwania po awarii możesz utworzyć i skonfigurować następująco:

- Utwórz plan ochrony zawierający moduł odzyskiwania po awarii i zastosuj go do swoich urządzeń. W ten sposób zostanie automatycznie utworzona domyślna infrastruktura odzyskiwania po awarii. Zobacz Tworzenie planu ochrony na potrzeby odzyskiwania po awarii.
- Ręcznie skonfiguruj chmurową infrastrukturę odzyskiwania po awarii, kontrolując każdy etap. Zobacz "Konfigurowanie serwerów odzyskiwania" (s. 835).

Najważniejsze funkcje

Uwaga
Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

- Zarządzanie usługą Cyber Disaster Recovery Cloud z jednej konsoli
- Możliwość rozszerzenia nawet 23 sieci lokalnych do chmury przy użyciu bezpiecznego tunelu VPN
- Nawiąż połączenie z lokalizacją w chmurze bez wdrażania urządzenia VPN (tryb Tylko chmura)
- Nawiąż połączenie point-to-site z lokalizacją lokalną i lokalizacją w chmurze
- Ochrona komputerów za pomocą serwerów odzyskiwania w chmurze
- Ochrona aplikacji i urządzeń za pomocą serwerów podstawowych w chmurze
- Automatyczne operacje odzyskiwania po awarii w przypadku szyfrowanych kopii zapasowych
- Testowanie przełączania awaryjnego w odizolowanej sieci
- Skorzystaj z runbooków, aby szybko przygotować środowisko produkcyjne w chmurze

© Acronis International GmbH, 2003-2024

Wymagania dotyczące oprogramowania

Obsługiwane systemy operacyjne

Ochrona za pomocą serwera odzyskiwania została przetestowana dla następujących systemów operacyjnych:

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Oprogramowanie może działać na innych systemach operacyjnych Windows oraz dystrybucjach systemu Linux, jednak nie jest to gwarantowane.

Uwaga
Ochrona z zastosowaniem serwera odzyskiwania została przetestowana w przypadku maszyn wirtualnych Microsoft Azure z następującymi systemami operacyjnymi:

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Ubuntu Server 20.04 LTS — Gen2 (firmy Canonical) Dodatkowe informacje na temat uzyskiwania dostępu do konsoli serwera odzyskiwania można znaleźć w artykule https://kb.acronis.com/content/71616.

Obsługiwane platformy wirtualizacji

Ochrona maszyn wirtualnych za pomocą serwera odzyskiwania została przetestowana dla następujących platform wirtualizacji:

© Acronis International GmbH, 2003-2024

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 z rolą Hyper-V
- Windows Server 2012/2012 R2 z rolą Hyper-V
- Windows Server 2016 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Maszyny wirtualne oparte na jądrze (KVM) — tylko w pełni zwirtualizowane maszyny-goście (HVM). Parawirtualne maszyny-goście (PV) nie są obsługiwane.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

Urządzenie VPN zostało przetestowane dla następujących platform wirtualizacji:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 z rolą Hyper-V
- Windows Server 2012/2012 R2 z rolą Hyper-V
- Windows Server 2016 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Oprogramowanie może działać na innych platformach wirtualizacji lub innych wersjach tych platform, jednak nie jest to gwarantowane.

Ograniczenia

W ramach usługi Cyber Disaster Recovery Cloud nie są obsługiwane następujące platformy i konfiguracje:

© Acronis International GmbH, 2003-2024

1. Nieobsługiwane platformy:
   - Agenty dla Virtuozzo
   - macOS
   - Systemy operacyjne Windows dla komputerów stacjonarnych nie są obsługiwane w związku z warunkami korzystania z produktów firmy Microsoft.
   - Wersja Windows Server Azure

     Wersja Azure to wersja systemu Windows Server opracowana specjalnie pod kątem działania jako maszyna wirtualna (VM) Azure IaaS na platformie Azure lub jako maszyna wirtualna w klastrze Azure Stack HCI. Wersja Azure — w odróżnieniu od wersji Standard i Datacenter — nie jest licencjonowana do działania na sprzęcie bez systemu operacyjnego, kliencie Windows Hyper-V, Windows Server Hyper-V, hiperwizorach innych firm ani w chmurach innych firm.
2. Nieobsługiwane konfiguracje:

   Microsoft Windows
   - Dyski dynamiczne nie są obsługiwane
   - Systemy operacyjne Windows dla komputerów stacjonarnych nie są obsługiwane (w związku z warunkami korzystania z produktów firmy Microsoft)
   - Usługa Active Directory z replikacją FRS nie jest obsługiwana
   - Nośniki wymienne bez formatowania GPT lub MBR (tzw. superdyskietki) nie są obsługiwane

   Linux
   - Systemy plików bez tabeli partycji
   - Obciążenia systemu Linux, których kopie zapasowe są tworzone za pomocą agenta z systemu operacyjnego gościa i które mają woluminy z następującymi zaawansowanymi konfiguracjami narzędzia Logical Volume Manager (LVM): Woluminy rozłożone, woluminy dublowane, RAID 0, RAID 4, RAID 5, RAID 6 lub RAID 10.

   Uwaga
   Obciążenia, na których zainstalowano więcej niż jeden system operacyjny, nie są obsługiwane.

3. Nieobsługiwane typy kopii zapasowych:
   - Punkty odzyskiwania tworzone w ramach ciągłej ochrony danych są niekompatybilne.

     Ważne
     Jeśli utworzysz serwer odzyskiwania na podstawie kopii zapasowej mającej punkt odzyskiwania utworzony w ramach ciągłej ochrony danych, to podczas powrotu po awarii lub tworzenia kopii zapasowej serwera odzyskiwania utracisz dane zawarte w tym punkcie.
   - Kopii zapasowych z danymi do analizy śledczej nie można używać do tworzenia serwerów odzyskiwania.

Serwer odzyskiwania ma jeden interfejs sieciowy. Jeśli pierwotna maszyna ma kilka interfejsów sieciowych, emulowany jest tylko jeden interfejs.

Serwery chmurowe nie są szyfrowane.

© Acronis International GmbH, 2003-2024

Wersja próbna rozwiązania Cyber Disaster Recovery Cloud

Z wersji próbnej rozwiązania Acronis Cyber Disaster Recovery Cloud można korzystać przez 30 dni. W okresie tym w rozwiązaniu Disaster Recovery występują następujące ograniczenia dla dzierżawców-partnerów:

- Serwery odzyskiwania i podstawowych nie mają dostępu do publicznego Internetu. Nie można przypisać tym serwerom publicznych adresów IP.
- Połączenie IPsec VPN multi-site jest niedostępne.

Ograniczenia w przypadku korzystania z magazynu Geo-redundant Cloud Storage

Geo-redundant Cloud Storage stanowi lokalizację dodatkową na potrzeby danych kopii zapasowych. Lokalizacja dodatkowa znajduje się w regionie, który jest geograficznie oddalony od lokalizacji głównego magazynu. Geograficzna separacja regionów gwarantuje, że jeśli w jednym z regionów dojdzie do katastrofalnych wydarzeń uniemożliwiających odzyskanie danych z kopii zapasowej, drugiego regionu nie będą one dotyczyć i będzie można kontynuować wszelkie operacje.

Ważne
Usługa Odzyskiwanie po awarii nie jest obsługiwana, jeśli lokalizacja magazynu kopii zapasowych zostanie zmieniona z lokalizacji podstawowej na lokalizację dodatkową cechującą się geograficzną nadmiarowością.

Kompatybilność modułu Odzyskiwanie po awarii z programami szyfrującymi

Moduł Odzyskiwanie po awarii jest kompatybilny z następującymi programami szyfrującymi na poziomie dysku:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

© Acronis International GmbH, 2003-2024

Uwaga

- W przypadku obciążeń z zastosowanym szyfrowaniem na poziomie dysku zalecamy zainstalowanie agenta ochrony w systemie operacyjnym gościa obciążenia i wykonywanie kopii zapasowych przy użyciu agenta.
- Przełączanie awaryjne i powrót po awarii nie będą obsługiwane w przypadku bezagentowych kopii zapasowych zaszyfrowanych obciążeń.

Aby uzyskać więcej informacji na temat kompatybilności oprogramowania Cyber Protection z oprogramowaniem szyfrującym, zobacz sekcję "Kompatybilność z programami szyfrującymi" (s. 44).

Punkty obliczeniowe

W usłudze Disaster Recovery punkty obliczeniowe są używane w przypadku serwerów podstawowych oraz serwerów odzyskiwania podczas testowego i produkcyjnego przełączania awaryjnego. Punkty obliczeniowe odzwierciedlają zasoby obliczeniowe używane do uruchamiania serwerów (maszyn wirtualnych) w chmurze.

Wykorzystanie punktów obliczeniowych podczas odzyskiwania po awarii zależy od parametrów serwera oraz czasu znajdowania się serwera w stanie przełączania awaryjnego. Im wydajniejszy jest serwer i im dłuższy jest ten czas, tym więcej punktów obliczeniowych zostanie wykorzystanych. A im więcej punktów obliczeniowych zostanie wykorzystanych, tym wyższe zostaną naliczone koszty.

W przypadku wszystkich serwerów działających w środowisku Acronis Cloud będą pobierane opłaty za punkty obliczeniowe — w zależności od ich skonfigurowanego wariantu, a niezależnie od ich stanu (włączone czy wyłączone).

Serwery odzyskiwania w stanie gotowości nie wykorzystują punktów obliczeniowych i nie będą za nie pobierane opłaty.

W poniższej tabeli znajduje się przykład ośmiu serwerów w chmurze w różnych wariantach oraz odpowiednie punkty obliczeniowe, które te serwery będą wykorzystywać w ciągu godziny. Warianty serwerów można zmieniać na karcie **Szczegóły**.

Typ	Procesor	Pamięć RAM	Punkty obliczeniowe
W1	1 procesor wirtualny	2 GB	1
F2	1 procesor wirtualny	4 GB	2
W3	2 procesory wirtualne	8 GB	4
W4	4 procesory wirtualne	16 GB	8
W5	8 procesorów wirtualnych	32 GB	16
W6	16 procesorów wirtualnych	64 GB	32
W7	16 procesorów wirtualnych	128 GB	64

© Acronis International GmbH, 2003-2024

Typ	Procesor	Pamięć RAM	Punkty obliczeniowe
W8	16 procesorów wirtualnych	256 GB	128

Dzięki informacjom z tabeli można łatwo oszacować, ile punktów obliczeniowych wykorzysta serwer (maszyna wirtualna).

Jeśli na przykład za pomocą usługi Odzyskiwanie po awarii ma być chroniona jedna maszyna wirtualna z 4 procesorami wirtualnymi* i 16 GB pamięci RAM oraz jedna maszyna wirtualna z 2 procesorami wirtualnymi i 8 GB pamięci RAM, pierwsza maszyna wirtualna wykorzysta 8 punktów obliczeniowych na godzinę, a druga — 4 punkty obliczeniowe na godzinę. Jeśli obie maszyny wirtualne znajdują się w stanie przełączania awaryjnego, łączne wykorzystanie osiągnie poziom 12 punktów obliczeniowych na godzinę lub 288 punktów obliczeniowych na cały dzień (12 punktów obliczeniowych na godzinę x 24 godziny = 288 punktów obliczeniowych).

* Pojęcie „procesor wirtualny" (vCPU) oznacza procesor fizyczny przypisany do maszyny wirtualnej i jest jednostką zależną od czasu.

Uwaga
W przypadku wykorzystania nadwyżki limitu **punktów obliczeniowych** wszystkie serwery podstawowe i serwery odzyskiwania zostaną wyłączone. Korzystanie z tych serwerów będzie możliwe dopiero po rozpoczęciu następnego okresu rozliczeniowego lub zwiększeniu limitu. Domyślnym okresem rozliczeniowym jest cały miesiąc kalendarzowy.

Konfigurowanie funkcji odzyskiwania po awarii

Uwaga
Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Aby skonfigurować funkcję odzyskiwania po awarii

1. Skonfiguruj typ łączności z lokalizacją w chmurze:
   - Połączenie point-to-site
   - Połączenie OpenVPN site-to-site
   - Połączenie IPsec VPN multi-site
   - Tryb Tylko chmura
2. Utwórz plan ochrony przy włączonym module kopii zapasowej i wybierz cały komputer lub system oraz woluminy startowe do uwzględnienia w kopii zapasowej. Do utworzenia serwera odzyskiwania wymagany jest co najmniej jeden plan ochrony.
3. Zastosuj plan ochrony do lokalnych serwerów, które mają być chronione.
4. Utwórz serwer odzyskiwania dla każdego lokalnego serwera, który chcesz chronić.

© Acronis International GmbH, 2003-2024

5. Wykonaj próbne przełączenie awaryjne, aby sprawdzić, jak działa.
6. [Opcjonalnie] Utwórz serwery podstawowe na potrzeby replikowania aplikacji.

W rezultacie zostanie skonfigurowana funkcja odzyskiwania po awarii w celu ochrony lokalnych serwerów przed skutkami awarii.

W razie wystąpienia awarii można wykonać przełączenie awaryjne obciążenia na serwery odzyskiwania w chmurze. Przed przełączeniem awaryjnym na serwery odzyskiwania musi zostać utworzony co najmniej jeden punkt odzyskiwania. Po usunięciu awarii w lokalizacji lokalnej można z powrotem przenieść do niej obciążenie, wykonując operację powrotu po awarii. Dodatkowe informacje na temat procesu powrotu po awarii można znaleźć w sekcjach "Wymagania wstępne" (s. 849) i "Wymagania wstępne" (s. 854).

Tworzenie planu ochrony na potrzeby odzyskiwania po awarii

Utwórz plan ochrony obejmujący moduł Odzyskiwanie po awarii i zastosuj go do swoich urządzeń.

W przypadku tworzenia nowego planu ochrony moduł Odzyskiwanie po awarii jest domyślnie wyłączony. Po włączeniu funkcji odzyskiwania po awarii i zastosowaniu planu do urządzeń tworzona jest infrastruktura sieci w chmurze, w tym *serwer odzyskiwania* dla każdego chronionego urządzenia. *Serwer odzyskiwania* to komputer wirtualny w chmurze będący kopią wybranego urządzenia. W przypadku każdego z wybranych urządzeń tworzony jest serwer odzyskiwania w stanie gotowości (bez uruchomienia maszyny wirtualnej) z ustawieniami domyślnymi. Rozmiar serwera odzyskiwania jest dobierany automatycznie — z uwzględnieniem procesora i pamięci RAM chronionego urządzenia. Domyślnie jest też automatycznie tworzona infrastruktura sieci w chmurze: Brama VPN i sieci w lokalizacji w chmurze, z którymi będą połączone serwery odzyskiwania.

Po odwołaniu, usunięciu lub wyłączeniu modułu Odzyskiwanie po awarii z planu ochrony serwery odzyskiwania i sieci w chmurze nie zostaną automatycznie usunięte. W razie potrzeby infrastrukturę odzyskiwania po awarii można usunąć ręcznie.

© Acronis International GmbH, 2003-2024

Uwaga

- Po skonfigurowaniu funkcji odzyskiwania po awarii będziesz mieć możliwość wykonania testowego lub produkcyjnego przełączenia awaryjnego z dowolnego z punktów odzyskiwania wygenerowanych po utworzeniu serwera odzyskiwania dla urządzenia. Punktów odzyskiwania wygenerowanych przed aktywowaniem ochrony urządzenia za pomocą funkcji odzyskiwania po awarii (tj. przed utworzeniem serwera odzyskiwania), nie można użyć do wykonania przełączenia awaryjnego.
- Jeśli nie uda się wykryć adresu IP urządzenia, to nie będzie można włączyć planu ochrony na potrzeby odzyskiwania po awarii. Może tak się zdarzyć na przykład w przypadku, gdy kopie zapasowe maszyn wirtualnych są tworzone bez agentów i maszyny nie mają przypisanych adresów IP.
- Po zastosowaniu planu ochrony w lokalizacji w chmurze są przypisywane te same sieci i adresy IP. Łączność IPsec VPN wymaga, aby segmenty sieci w lokalizacjach w chmurze i lokalnych się nie pokrywały. Jeśli skonfigurowano łączność IPsec VPN multi-site, a następnie zastosowano plan ochrony do jednego lub kilku urządzeń, należy dodatkowo zaktualizować sieci w chmurze i ponownie przypisać adresy IP serwerów chmurowych. Aby uzyskać więcej informacji, zobacz "Zmienianie przypisania adresów IP" (s. 825).

Aby utworzyć plan ochrony na potrzeby odzyskiwania po awarii

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputery, które chcesz chronić.
3. Kliknij **Chroń**, a następnie kliknij **Utwórz plan**.
   Zostanie otwarta sekcja domyślnych ustawień planu ochrony.
4. Skonfiguruj opcje kopii zapasowej.
   Aby korzystać z funkcji odzyskiwania po awarii ramach planu w chmurze musi zostać utworzona kopia zapasowa całego komputera lub tylko dysków niezbędnych do uruchomienia komputera i udostępnienia potrzebnych usług.
5. Włącz moduł Odzyskiwanie po awarii, klikając przełącznik obok jego nazwy.
6. Kliknij **Utwórz**.
   Plan zostanie utworzony i zastosowany do wybranych komputerów.

Co dalej

- Domyślną konfigurację serwera odzyskiwania można edytować. Aby uzyskać więcej informacji, zobacz "Konfigurowanie serwerów odzyskiwania" (s. 835).
- Domyślną konfigurację sieci można edytować. Aby uzyskać więcej informacji, zobacz "Konfigurowanie łączności" (s. 797).
- Można znaleźć więcej informacji na temat domyślnych parametrów serwerów odzyskiwania i infrastruktury sieci w chmurze. Dodatkowe informacje można znaleźć w sekcjach "Edytowanie domyślnych parametrów serwera odzyskiwania" (s. 795) i "Infrastruktura sieci w chmurze" (s. 796).

© Acronis International GmbH, 2003-2024

Edytowanie domyślnych parametrów serwera odzyskiwania

Podczas tworzenia i stosowania planu ochrony na potrzeby odzyskiwania po awarii jest tworzony serwer odzyskiwania z parametrami domyślnymi. Te domyślne parametry można później edytować.

Uwaga
Serwer odzyskiwania jest tworzony tylko wtedy, jeśli jeszcze go nie ma. Istniejące już serwery odzyskiwania nie są zmieniane ani tworzone ponownie.

Aby edytować domyślne parametry serwera odzyskiwania

1. Przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz urządzenie i kliknij **Odzyskiwanie po awarii**.
3. Edytuj domyślne parametry serwera odzyskiwania.
   Parametry serwera odzyskiwania zostały opisane w poniższej tabeli.

Serwer odzyskiwania parametr	**Domyślne wartość**	**Opis**
Procesor i pamięć RAM	automatycznie	Wybierz liczbę procesorów wirtualnych i rozmiar pamięci RAM serwera odzyskiwania. Ustawienia domyślne zostaną określone automatycznie na podstawie oryginalnej konfiguracji procesora i pamięci RAM urządzenia.
Sieć w chmurze	automatycznie	Sieć w chmurze, do której ma zostać podłączony serwer. Szczegółowe informacje na temat konfigurowania sieci w chmurze można znaleźć w sekcji Infrastruktura sieci w chmurze.
Adres IP w sieci produkcyjnej	automatycznie	Adres IP, który serwer będzie mieć przypisany w sieci produkcyjnej. Domyślnie używany jest adres IP pierwotnego komputera.
Testowy adres IP	wyłączone	Testowy adres IP umożliwia przetestowanie przełączania awaryjnego w odizolowanej sieci testowej i połączenie serwera odzyskiwania przy użyciu protokołu RDP lub SSH podczas testu przełączania awaryjnego. W trybie testowego przełączania awaryjnego brama VPN zastępuje testowy adres IP produkcyjnym adresem IP za pomocą protokołu NAT. Jeśli testowy adres IP nie zostanie określony, dostęp do serwera będzie możliwy wyłącznie z poziomu konsoli.
Dostęp do	włączone	Włącz dostęp serwera odzyskiwania do Internetu

© Acronis International GmbH, 2003-2024

Internetu		podczas prawdziwego lub testowego przełączania awaryjnego. Domyślnie w przypadku portu TCP 25 jest skonfigurowana odmowa połączeń wychodzących.
Użyj adresu publicznego	wyłączone	Publiczny adres IP serwera czyni go dostępnym w Internecie podczas prawdziwego lub testowego przełączania awaryjnego. Jeśli nie użyjesz publicznego adresu IP, serwer będzie dostępny wyłącznie w Twojej sieci produkcyjnej. Aby użyć publicznego adresu IP, należy włączyć dostęp do Internetu. Publiczny adres IP zostanie wyświetlony po zakończeniu konfiguracji. Domyślnie port TCP 443 jest otwarty dla połączeń przychodzących.
Ustaw próg RPO	wyłączone	Próg RPO określa maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania a czasem bieżącym. Można ustawić wartość z przedziałów: 15– 60 minut, 1–24 godz., 1–14 dni.

Infrastruktura sieci w chmurze

Infrastruktura sieci w chmurze składa się z bramy VPN w lokalizacji w chmurze oraz sieci w chmurze, z którymi będą połączone serwery odzyskiwania.

Uwaga
Zastosowanie planu ochrony na potrzeby odzyskiwania po awarii powoduje utworzenie infrastruktury sieci w chmurze do odzyskiwania tylko wtedy, gdy takiej infrastruktury jeszcze nie ma. Istniejące już sieci w chmurze nie są zmieniane ani tworzone ponownie.

System sprawdza adresy IP urządzeń i jeśli nie ma jeszcze sieci w chmurze, do której pasuje dany adres IP, zostanie ona automatycznie utworzona. Jeśli zaś istnieje już sieć w chmurze, do której pasuje adres IP serwera odzyskiwania, sieć ta nie jest zmieniana ani tworzona ponownie.

- Jeśli jeszcze nie ma sieci w chmurze lub ustawienia odzyskiwania po awarii są konfigurowane po raz pierwszy, sieci w chmurze zostaną utworzone z maksymalnymi zakresami zalecanymi przez IANA do użytku prywatnego (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) na podstawie zakresu adresów IP urządzeń. Sieć można zawęzić, edytując jej maskę.
- Jeśli masz urządzenia w wielu sieciach lokalnych, sieć w chmurze może stać się obszarem nadrzędnym w stosunku do sieci lokalnych. Konfiguracje sieci można zmieniać w sekcji **Łączność**. Zobacz "Zarządzanie sieciami" (s. 818).
- W razie konieczności skonfigurowania połączenia Open VPN site-to-site pobierz urządzenie VPN i je skonfiguruj. Zobacz "Konfigurowanie połączenia Open VPN site-to-site" (s. 808). Upewnij się, że zakresy sieci w chmurze odpowiadają zakresom sieci lokalnych podłączonych do urządzenia VPN.

© Acronis International GmbH, 2003-2024

- Aby zmienić domyślną konfigurację sieci, kliknij łącze **Przejdź do sekcji łączności** w module Disaster Recovery planu ochrony lub kliknij **Odzyskiwanie po awarii** > **Łączność**.

Konfigurowanie łączności

W tej sekcji omówiono zagadnienia sieciowe niezbędne do zrozumienia działania wszystkich elementów w ramach usługi Cyber Disaster Recovery Cloud. Dowiesz się, jak skonfigurować różne rodzaje łączności z lokalizacją w chmurze — stosownie do potrzeb. Dowiesz się też, jak należy zarządzać sieciami w chmurze oraz konfigurować ustawienia urządzenia VPN i bramy VPN.

Pojęcia dotyczące sieci

Uwaga
Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Za pomocą usługi Cyber Disaster Recovery Cloud można zdefiniować następujące typy łączności z lokalizacją w chmurze:

- **Tryb Tylko chmura**

  Połączenie tego typu nie wymaga wdrożenia urządzenia VPN w lokalizacji lokalnej.

  Sieć lokalna i sieć w chmurze działają niezależnie. Ten typ połączenia oznacza albo przełączenie awaryjne wszystkich chronionych serwerów z lokalizacji lokalnej, albo częściowe przełączenie awaryjne niezależnych serwerów, które nie muszą się komunikować z lokalizacją lokalną.

  Serwery chmurowe w lokalizacji w chmurze są dostępne przez sieć lokalną, połączenie VPN point-to-site i publiczne adresy IP (jeśli zostały przypisane).
- **Połączenie Open VPN site-to-site**

  Połączenie tego typu wymaga wdrożenia urządzenia VPN w lokalizacji lokalnej.

  Połączenie Open VPN site-to-site pozwala na rozszerzenie sieci na chmurę z zachowaniem adresów IP.

  Lokalizacja lokalna zostaje połączona z lokalizacją w chmurze za pomocą bezpiecznego tunelu VPN. Ten typ połączenia jest odpowiedni w sytuacji, gdy w lokalizacji lokalnej występują mocno zależne serwery, takie jak serwer internetowy czy serwer bazy danych. W przypadku częściowego przełączenia awaryjnego — gdy jeden z serwerów jest odtwarzany w lokalizacji w chmurze, a drugi pozostaje w lokalizacji lokalnej — będą one mogły nadal się ze sobą komunikować przez tunel VPN.

  Serwery chmurowe w lokalizacji w chmurze są dostępne przez sieć lokalną, połączenie VPN point-to-site i publiczne adresy IP (jeśli zostały przypisane).
- **Połączenie IPsec VPN multi-site**

  Połączenie tego typu wymaga lokalnego urządzenia VPN, które obsługuje protokół IPsec IKE v2.

  Gdy zaczniesz konfigurować połączenie IPsec VPN multi-site, usługa Cyber Disaster Recovery Cloud automatycznie utworzy chmurową bramę VPN z publicznym adresem IP.

© Acronis International GmbH, 2003-2024

Dzięki połączeniu IPsec VPN multi-site lokalizacje lokalne zostają połączone z lokalizacją w chmurze za pomocą bezpiecznego tunelu VPN.

Połączenie tego typu jest odpowiednie w scenariuszach usługi Disaster Recovery z jedną lub kilkoma lokalizacjami lokalnymi hostującymi obciążenia krytyczne lub ściśle zależne usługi.

W przypadku częściowego przełączenia awaryjnego jednego z serwerów serwer ten jest odtwarzany w lokalizacji w chmurze, a pozostałe serwery pozostają w lokalizacji lokalnej — będą one mogły nadal się ze sobą komunikować przez tunel IPsec VPN.

W przypadku częściowego przełączenia awaryjnego jednej z lokalizacji lokalnych pozostałe lokalizacje lokalne działają i będą mogły nadal się ze sobą komunikować przez tunel IPsec VPN.

- **Zdalny dostęp VPN point-to-site**

  Bezpieczny zdalny dostęp VPN point-to-site do własnych obciążeń w lokalizacji w chmurze i lokalizacji lokalnej z zewnątrz za pomocą własnego urządzenia końcowego.

  Aby uzyskać dostęp do lokalizacji lokalnej przy użyciu połączenia tego typu, trzeba wdrożyć w niej urządzenie VPN.

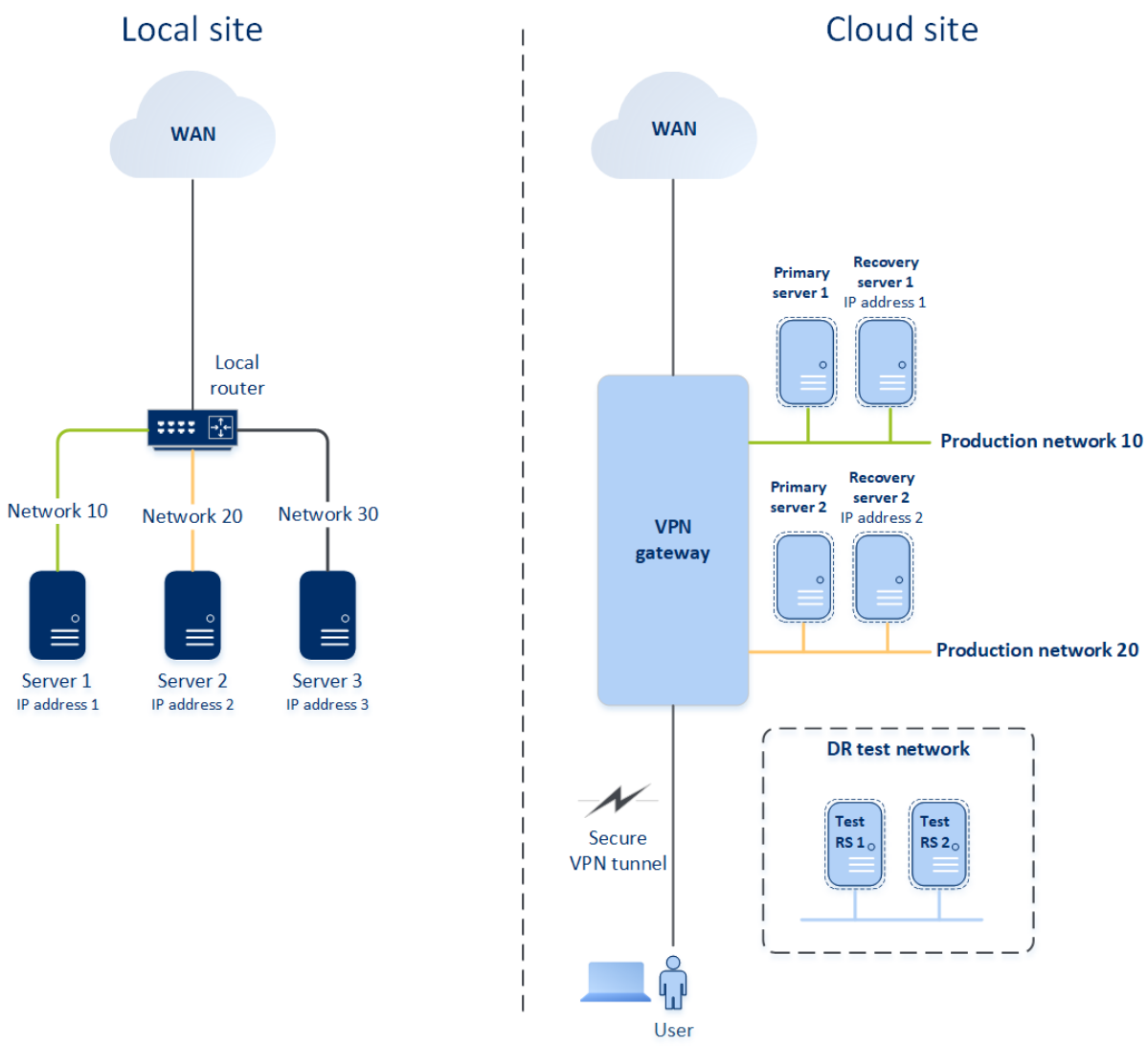
Tryb Tylko chmura

Tryb Tylko chmura nie wymaga wdrożenia urządzenia VPN w lokalizacji lokalnej. Oznacza to dwie niezależne sieci: jedną w lokalizacji lokalnej, drugą w lokalizacji w chmurze. Routing jest obsługiwany przez router w lokalizacji w chmurze.

Jak działa routing

W przypadku ustanowienia trybu Tylko chmura routing jest obsługiwany przez router w lokalizacji w chmurze, dzięki czemu mogą się ze sobą komunikować serwery z różnych sieci w chmurze.

© Acronis International GmbH, 2003-2024



Połączenie Open VPN site-to-site

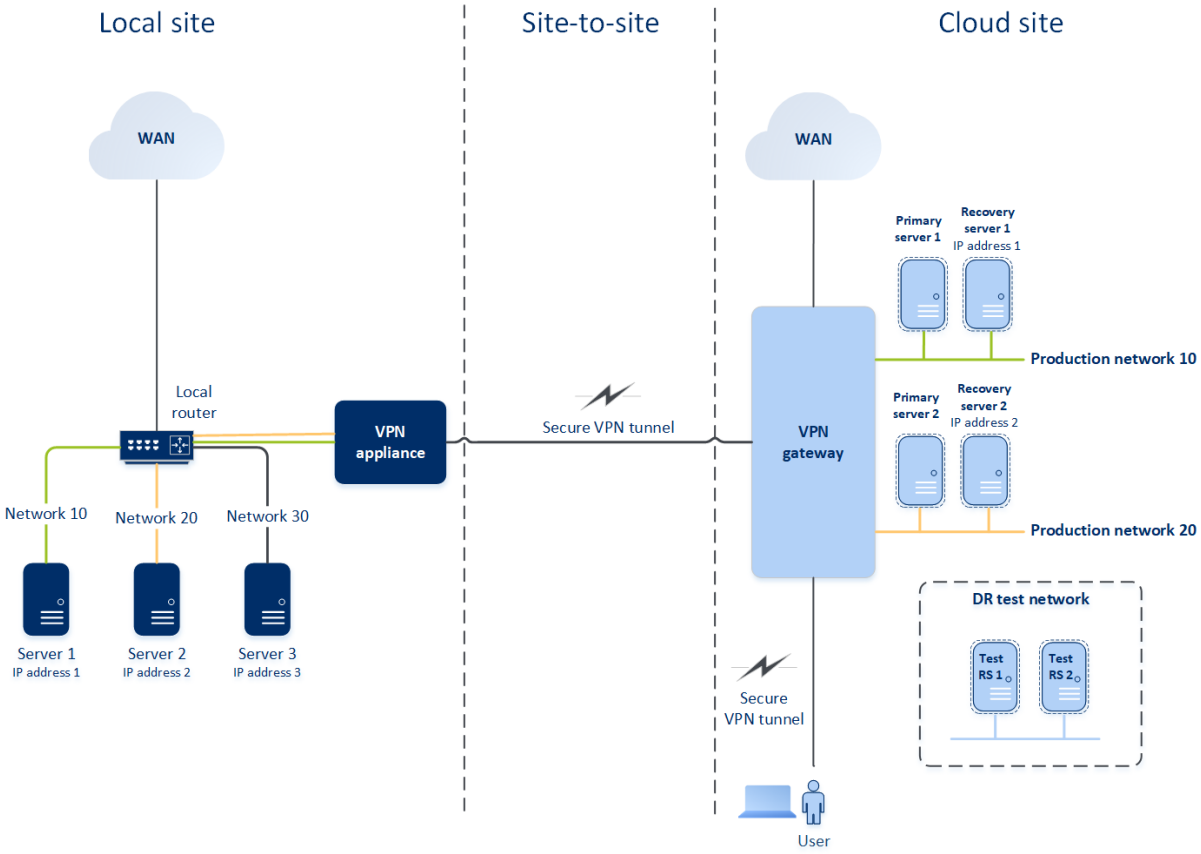
Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Aby przedstawić, jak działają sieci w ramach usługi Cyber Disaster Recovery Cloud, posłużymy się przykładem lokalizacji lokalnej, w której znajdują się trzy sieci z jednym komputerem w każdej z nich. Skonfigurujesz ochronę przed awarią w przypadku dwóch z tych sieci — Network 10 i Network 20.

Na poniższym diagramie widać lokalizację lokalną, w której są hostowane komputery, i lokalizację w chmurze, w której w razie awarii są uruchamiane serwery chmurowe.

Usługa Cyber Disaster Recovery Cloud pozwala na przełączenie awaryjne wszystkich obciążeń z uszkodzonych komputerów w lokalizacji lokalnej na serwery chmurowe w chmurze. Za pomocą usługi Cyber Disaster Recovery Cloud można chronić do 23 sieci.

© Acronis International GmbH, 2003-2024



Do komunikacji Open VPN site-to-site między lokalizacją lokalną i lokalizacją w chmurze służy **urządzenie VPN** i **brama VPN**. Gdy zaczniesz konfigurować połączenie Open VPN site-to-site w konsoli Cyber Protect, w lokalizacji w chmurze automatycznie zostanie wdrożona brama VPN. Następnie trzeba wdrożyć urządzenie VPN w lokalizacji lokalnej, dodać sieci, które mają być chronione, i zarejestrować urządzenie w chmurze. Usługa Cyber Disaster Recovery Cloud utworzy w chmurze replikę sieci lokalnej. Między urządzeniem VPN a bramą VPN jest tworzony bezpieczny tunel VPN. Oznacza on rozszerzenie sieci lokalnej o chmurę. Sieci produkcyjne w chmurze są połączone z sieciami lokalnymi. Serwery lokalne i chmurowe mogą się komunikować przez ten tunel VPN tak, jakby znajdowały się w tym samym segmencie sieci Ethernet. Routing jest obsługiwany przez lokalny router.

Dla każdego komputera źródłowego, który ma być chroniony, trzeba utworzyć serwer odzyskiwania w lokalizacji w chmurze. Dopóki nie nastąpi przełączenie awaryjne, działa on w **trybie gotowości**. Jeśli dojdzie do awarii i uruchomisz proces przełączania awaryjnego (w **trybie produkcyjnym**), w chmurze zostanie uruchomiony serwer odzyskiwania stanowiący dokładną kopię chronionego komputera. Może on mieć przypisany ten sam adres IP, który ma komputer źródłowy, i zostać uruchomiony w tym samym segmencie sieci Ethernet. Klienci nadal mogą korzystać z serwera, nie zauważając żadnych zmian zachodzących w tle.

Proces przełączania awaryjnego można też uruchomić w **trybie testowym**. Oznacza on, że komputer źródłowy nadal działa, a jednocześnie w chmurze zostaje uruchomiony odpowiedni serwer odzyskiwania o tym samym adresie IP. Aby zapobiec konfliktom adresów IP, w chmurze jest tworzona specjalna sieć wirtualna — **sieć testowa**. Sieć testowa jest odizolowana w celu

© Acronis International GmbH, 2003-2024

zapobieżenia zdublowaniu adresu IP komputera źródłowego w tym samym segmencie sieci Ethernet. Aby uzyskać dostęp do serwera odzyskiwania w trybie testowego przełączenia awaryjnego, podczas tworzenia tego serwera trzeba mu przypisać **Testowy adres IP**. Istnieją też inne parametry serwera odzyskiwania, które można zdefiniować — zostały one omówione w dalszej części dokumentu.

Jak działa routing

W przypadku nawiązania połączenia site-to-site routing między sieciami w chmurze jest obsługiwany przez router lokalny. Serwer VPN nie obsługuje routingu między serwerami chmurowymi znajdującymi się w różnych sieciach w chmurze. Jeśli serwer chmurowy z jednej sieci spróbuje się skomunikować z serwerem z innej sieci w chmurze, ruch przechodzi przez tunel VPN do routera lokalnego w lokalizacji lokalnej. Następnie router lokalny kieruje ruch do innej sieci, po czym ruch wraca przez tunel do serwera docelowego w lokalizacji w chmurze.

Brama VPN

Ważnym komponentem, który umożliwia komunikację między lokalizacją lokalną i lokalizacją w chmurze, jest **brama VPN**. Jest to maszyna wirtualna w chmurze z zainstalowanym specjalnym oprogramowaniem i szczególną konfiguracją sieci. Brama VPN pełni następujące funkcje:

- Łączy segmenty Ethernet sieci lokalnej i sieci produkcyjnej w chmurze w trybie L2.
- Udostępnia reguły iptables i ebtables.
- Stanowi domyślny router oraz NAT dla komputerów w sieciach testowych i produkcyjnych.
- Działa jako serwer DHCP. Wszystkie komputery w sieciach produkcyjnych i testowych muszą uzyskać konfigurację sieci (adresy IP, ustawienia DNS) przez DHCP. Serwer chmurowy za każdym razem otrzymuje od serwera DHCP ten sam adres IP. Jeśli zechcesz mieć własną konfigurację DNS, skontaktuj się z zespołem pomocy technicznej.
- Działa jako pamięć podręczna DNS.

Konfiguracja sieci bramy VPN

Brama VPN ma kilka interfejsów sieciowych:

- Interfejs zewnętrzny, połączony z Internetem
- Interfejsy produkcyjne, połączone z sieciami produkcyjnymi
- Interfejs testowy, połączony z siecią testową

Ponadto dodano dwa interfejsy wirtualne na potrzeby połączeń point-to-site i site-to-site.

Po wdrożeniu i zainicjowaniu bramy VPN tworzone są mostki: jeden dla interfejsu zewnętrznego, drugi dla interfejsu klienta i interfejsów produkcyjnych. Mimo że mostek interfejsów klienta i produkcyjnych oraz interfejs testowy używają tych samych adresów IP, brama VPN i tak jest w stanie prawidłowo kierować pakiety przy użyciu pewnej specjalnej techniki.

© Acronis International GmbH, 2003-2024

Urządzenie VPN

Urządzenie VPN to maszyna wirtualna w lokalizacji lokalnej z zainstalowanym systemem Linux i specjalnym oprogramowaniem oraz specjalną konfiguracją sieci. Umożliwia ono komunikację między lokalizacją lokalną i lokalizacją w chmurze.

Serwery odzyskiwania

Serwer odzyskiwania — replika oryginalnego komputera utworzona na podstawie przechowywanych w chmurze kopii zapasowych chronionego serwera. Serwery odzyskiwania służą do przełączania obciążeń z oryginalnych serwerów w razie wystąpienia awarii.

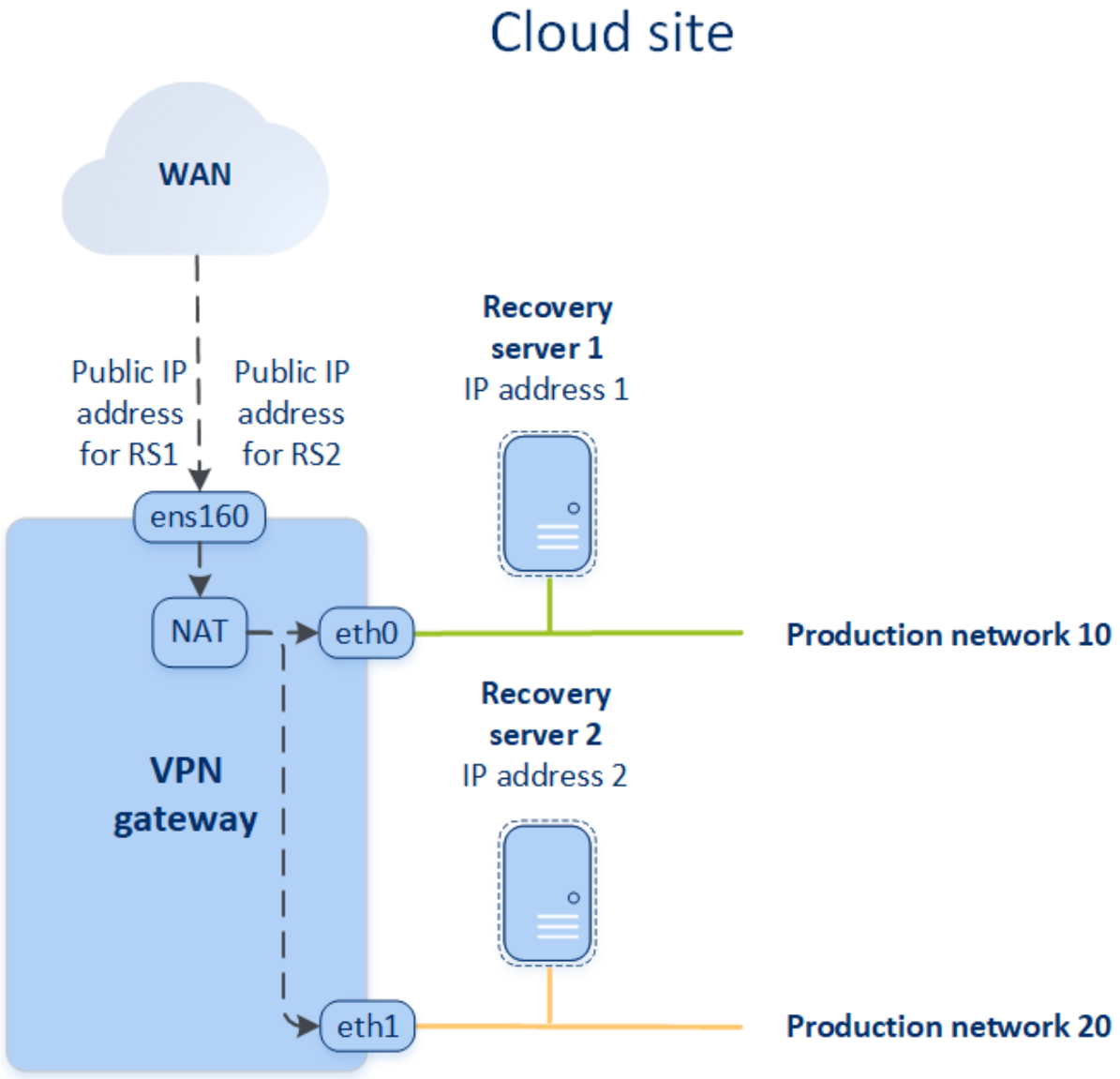
Podczas tworzenia serwera odzyskiwania trzeba określić następujące parametry sieciowe:

- **Sieć w chmurze** (wartość wymagana) — sieć w chmurze, do której zostanie podłączony serwer odzyskiwania.
- **Adres IP w sieci produkcyjnej** (wartość wymagana) — adres IP, z jakim zostanie uruchomiona maszyna wirtualna dla serwera odzyskiwania. Adres ten jest używany zarówno w sieciach produkcyjnych, jak i testowych. Przed uruchomieniem maszyna wirtualna zostaje skonfigurowana tak, aby uzyskała adres IP przez DHCP.
- **Testowy adres IP** (wartość opcjonalna) — adres IP potrzebny do uzyskania dostępu do serwera odzyskiwania z sieci produkcyjnej klienta podczas testowego przełączania awaryjnego, nadawany w celu zapobieżenia zdublowaniu produkcyjnego adresu IP w tej samej sieci. Ten adres IP różni się od adresu IP używanego w sieci produkcyjnej. Serwery w lokalizacji lokalnej mają dostęp do serwera odzyskiwania podczas testowego przełączania awaryjnego przy użyciu testowego adresu IP, podczas gdy dostęp w drugim kierunku nie jest możliwy. Jeśli podczas tworzenia serwera odzyskiwania została zaznaczona opcja **Dostęp do Internetu**, to można uzyskać dostęp do Internetu z serwera odzyskiwania znajdującego się w sieci testowej.
- **Publiczny adres IP** (wartość opcjonalna) — adres IP umożliwiający dostęp do serwera odzyskiwania z Internetu. Jeśli serwer nie ma publicznego adresu IP, można uzyskać do niego dostęp tylko z sieci lokalnej.
- **Dostęp do Internetu** (wartość opcjonalna) — aktywacja dostępu serwera odzyskiwania do Internetu (zarówno przy produkcyjnym, jak i testowym przełączaniu awaryjnym).

Publiczny i testowy adres IP

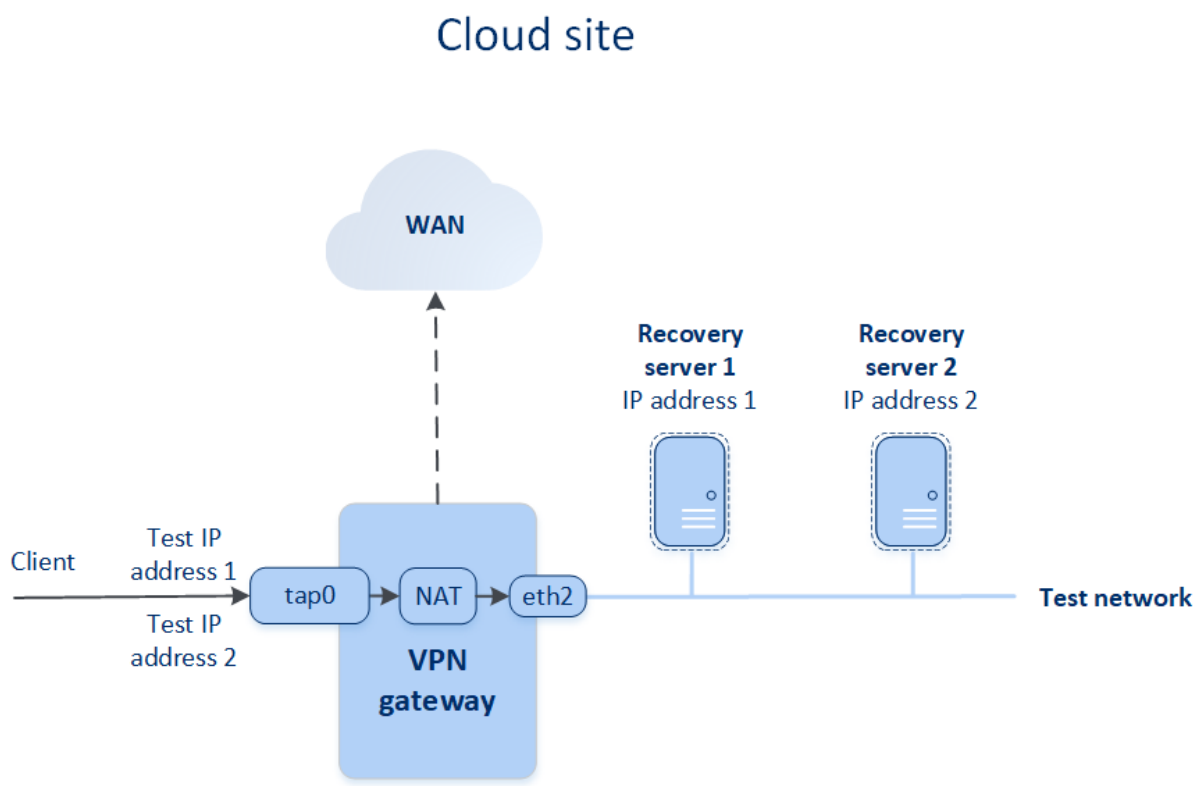
Jeśli podczas tworzenia serwera odzyskiwania zostanie mu przypisany publiczny adres IP, serwer ten będzie dostępny z Internetu przy użyciu tego adresu. Gdy z Internetu nadejdzie pakiet z publicznym adresem IP obiektu docelowego, brama VPN mapuje go na odpowiedni produkcyjny adres IP za pomocą usługi NAT i wysyła pakiet do odpowiadającego mu serwera odzyskiwania.

© Acronis International GmbH, 2003-2024



Jeśli podczas tworzenia serwera odzyskiwania zostanie mu przypisany testowy adres IP, serwer ten będzie dostępny w sieci testowej przy użyciu tego adresu. W przypadku wykonania testowego przełączenia awaryjnego oryginalny komputer nadal działa, a w sieci testowej w chmurze zostaje uruchomiony serwer odzyskiwania o tym samym adresie IP. Ponieważ sieć testowa jest odizolowana, nie występuje konflikt adresów IP. Serwery odzyskiwania w sieci testowej są dostępne przy użyciu ich testowych adresów IP, które są mapowane na produkcyjne adresy IP przez usługę NAT.

© Acronis International GmbH, 2003-2024



Dodatkowe informacje na temat połączeń VPN site-to-site: "Połączenie Open VPN site-to-site — dodatkowe informacje" (s. 198).

Serwery podstawowe

Serwer podstawowy — maszyna wirtualna, z którą nie jest powiązana żadna maszyna w lokalizacji lokalnej, w odróżnieniu od serwera odzyskiwania. Serwery podstawowe służą do ochrony aplikacji przy użyciu replikacji lub obsługi różnych usług pomocniczych (np. serwera internetowego).

Serwer główny jest najczęściej wykorzystywany w celu replikacji danych (w czasie rzeczywistym) ze wszystkich serwerów, na których uruchomione są kluczowe aplikacje. Replikację można ustawić samodzielnie za pomocą macierzystych narzędzi aplikacji. Na przykład replikacja Active Directory lub SQL może zostać skonfigurowana na potrzeby serwerów lokalnych oraz serwera podstawowego.

Serwer główny można też dołączyć do grupy AlwaysOn Availability Group (AAG) lub Database Availability Group (DAG).

Obie metody wymagają posiadania obszernej wiedzy na temat aplikacji oraz uprawnień administratora. Serwer główny nieustannie wykorzystuje zasoby obliczeniowe oraz miejsce w magazynie szybkiego odzyskiwania po awarii. Wymaga konserwacji ze strony użytkownika – monitorowania replikacji, instalowania aktualizacji oprogramowania, tworzenia kopii zapasowych. Korzyści serwera głównego to minimalne docelowe punkty i czasy odzyskiwania (RPO i RTO), obciążające środowisku produkcyjne w minimalnym stopniu (w porównaniu z metodą tworzenia w chmurze kopii zapasowych całych serwerów).

© Acronis International GmbH, 2003-2024

Serwery podstawowe zawsze są uruchamiane wyłącznie w sieci produkcyjnej i mają następujące parametry sieciowe:

- **Sieć w chmurze** (wartość wymagana) — sieć w chmurze, do której zostanie podłączony serwer podstawowy.
- **Adres IP w sieci produkcyjnej** (wartość wymagana) — adres IP serwera podstawowego w sieci produkcyjnej. Domyślnie wybierany jest pierwszy niezajęty adres IP w Twojej sieci produkcyjnej.
- **Publiczny adres IP** (wartość opcjonalna) — adres IP używany w celu uzyskania dostępu do serwera podstawowego z Internetu. Jeśli serwer nie ma publicznego adresu IP, można uzyskać do niego dostęp tylko z sieci lokalnej, a nie z Internetu.
- **Dostęp do Internetu** (wartość opcjonalna) — aktywacja dostępu serwera podstawowego do Internetu.

Połączenie IPsec VPN multi-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Połączenia IPsec VPN multi-site można użyć w celu połączenia jednej lub wielu lokalizacji lokalnych z usługą Cyber Disaster Recovery Cloud przez bezpieczne połączenie L3 IPsec VPN.

Łączność tego typu jest przydatna w scenariuszach usługi Disaster Recovery, jeśli występuje jedna z poniższych sytuacji:

- Masz jedną lokalizację lokalną hostującą krytyczne obciążenia.
- Masz wiele lokalizacji lokalnych hostujących krytyczne obciążenia, na przykład biura w różnych miejscach.
- korzystasz z lokalizacji oprogramowania innych firm lub lokalizacji dostawców usług zarządzanych i łączysz się z nimi za pośrednictwem tunelu IPsec VPN.

Do komunikacji IPsec VPN multi-site między lokalizacjami lokalnymi a lokalizacją w chmurze służy **brama VPN**. Gdy zaczniesz konfigurować połączenie IPsec VPN multi-site w konsoli Cyber Protect, w lokalizacji w chmurze automatycznie zostanie wdrożona brama VPN. Należy skonfigurować segmenty sieci w chmurze i dopilnować, aby nie pokrywały się z segmentami sieci lokalnej. Między lokalnymi lokalizacjami a lokalizacją w chmurze jest tworzony bezpieczny tunel VPN. Serwery lokalne i chmurowe mogą się komunikować przez ten tunel VPN tak, jakby znajdowały się w tym samym segmencie sieci Ethernet.

Dla każdego komputera źródłowego, który ma być chroniony, trzeba utworzyć serwer odzyskiwania w lokalizacji w chmurze. Dopóki nie nastąpi przełączenie awaryjne, działa on w **trybie gotowości**. Jeśli dojdzie do awarii i uruchomisz proces przełączania awaryjnego (w **trybie produkcyjnym**), w chmurze zostanie uruchomiony serwer odzyskiwania stanowiący dokładną kopię chronionego komputera. Klienci nadal mogą korzystać z serwera, nie zauważając żadnych zmian zachodzących w tle.

© Acronis International GmbH, 2003-2024

Proces przełączania awaryjnego można też uruchomić w **trybie testowym**. Oznacza on, że komputer źródłowy nadal działa, a jednocześnie w specjalnej sieci wirtualnej utworzonej w chmurze — **sieci testowej** — zostaje uruchomiony odpowiedni serwer odzyskiwania. Sieć testowa jest odizolowana w celu zapobieżenia duplikatom adresów IP w innych segmentach sieci w chmurze.

Brama VPN

Ważnym komponentem, który umożliwia komunikację między lokalizacjami lokalnymi a lokalizacją w chmurze, jest **brama VPN**. Jest to maszyna wirtualna w chmurze z zainstalowanym specjalnym oprogramowaniem i szczególną konfiguracją sieci. Brama VPN pełni następujące funkcje:

- Łączy segmenty Ethernet sieci lokalnej i sieci produkcyjnej w chmurze w trybie L3 IPsec.
- Stanowi domyślny router oraz NAT dla komputerów w sieciach testowych i produkcyjnych.
- Działa jako serwer DHCP. Wszystkie komputery w sieciach produkcyjnych i testowych muszą uzyskać konfigurację sieci (adresy IP, ustawienia DNS) przez DHCP. Serwer chmurowy za każdym razem otrzymuje od serwera DHCP ten sam adres IP.

  Jeśli wolisz, możesz zdefiniować niestandardową konfigurację DNS. Aby uzyskać więcej informacji, zobacz "Konfigurowanie niestandardowych serwerów DNS" (s. 826).
- Działa jako pamięć podręczna DNS.

Jak działa routing

Routing między sieciami w chmurze jest obsługiwany przez router w lokalizacji w chmurze, dzięki czemu mogą się ze sobą komunikować serwery z różnych sieci w chmurze.

Zdalny dostęp VPN point-to-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Połączenie point-to-site to bezpieczne połączenie z zewnątrz nawiązywane z urządzeń końcowych (np. komputera stacjonarnego lub laptopa) z lokalizacją lokalną lub lokalizacją w chmurze za pośrednictwem sieci VPN. Jest dostępne po nawiązaniu połączenia Open VPN site-to-site z lokalizacją Cyber Disaster Recovery Cloud. Połączenie tego typu jest przydatne w następujących przypadkach:

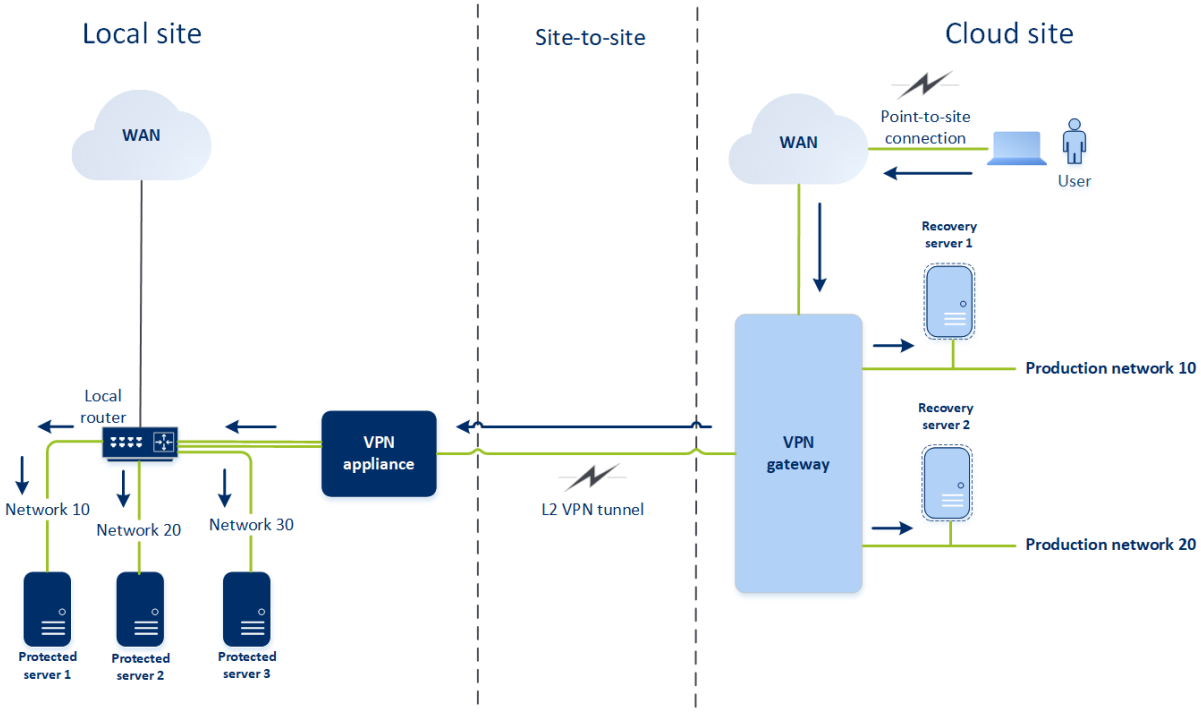
- W wielu firmach ich usługi i zasoby internetowe są dostępne tylko z firmowych sieci. Połączenie point-to-site umożliwia bezpieczne łączenie się z lokalizacją lokalną.
- W razie wystąpienia awarii, gdy obciążenie jest przenoszone do lokalizacji w chmurze, a sieć lokalna nie działa, może być konieczny bezpośredni dostęp do serwerów chmurowych. Jest to możliwe za pośrednictwem połączenia point-to-site z lokalizacją w chmurze.

W celu ustanowienia połączenia point-to-site z lokalizacją lokalną należy zainstalować w niej urządzenie VPN i skonfigurować połączenie site-to-site, a następnie połączenie point-to-site z

© Acronis International GmbH, 2003-2024

lokalizacją lokalną. Dzięki temu pracownicy zdalni będą mieli dostęp do firmowej sieci przez VPN warstwy 2 (L2 VPN).

Poniższy schemat przedstawia lokalizację lokalną, lokalizację w chmurze oraz komunikację między serwerami wyróżnioną kolorem zielonym. Tunel VPN warstwy 2 łączy lokalizację lokalną z lokalizacją w chmurze. Gdy użytkownik nawiąże połączenie point-to-site, komunikacja z lokalizacją lokalną odbywa się za pośrednictwem lokalizacji w chmurze.



W konfiguracji połączenia point-to-site do uwierzytelniania klienta VPN są używane certyfikaty. Dodatkowo do uwierzytelniania służą też poświadczenia użytkownika. Warto pamiętać o następujących kwestiach dotyczących połączenia point-to-site z lokalizacją lokalną:

- W celu uwierzytelnienia się w kliencie VPN użytkownicy powinni używać swoich poświadczeń z platformy Cyber Protect Cloud. Muszą też mieć przypisaną rolę użytkownika „Administrator firmy" lub „Cyber Protection".
- W razie ponownego utworzenia konfiguracji OpenVPN trzeba przekazać zaktualizowaną konfigurację wszystkim użytkownikom korzystającym z połączenia point-to-site z lokalizacją w chmurze.

Automatyczne usuwanie nieużywanych środowisk klientów w lokalizacji w chmurze

Disaster Recovery monitoruje wykorzystanie środowisk klientów utworzonych na potrzeby odzyskiwania po awarii i automatycznie je usuwa, jeśli nie są używane.

W celu ustalenia, czy dzierżawca-klient jest aktywny, są używane następujące kryteria:

© Acronis International GmbH, 2003-2024

- Co najmniej jeden serwer chmurowy istnieje obecnie lub istniał w ciągu ostatnich 7 dni.

  LUB

- Opcja **Dostęp VPN do lokalizacji lokalnej** jest włączona i albo został utworzony tunel Open VPN site-to-site, albo istnieją dane zgłoszone z urządzenia VPN dotyczące ostatnich 7 dni.

Pozostali dzierżawcy są uznawani za nieaktywnych. W przypadku takich dzierżawców system wykonuje następujące czynności:

- Usuwa bramę VPN i wszystkie zasoby chmury powiązane z danym dzierżawcą.
- Wyrejestrowuje urządzenie VPN.

W przypadku nieaktywnych dzierżawców przywracany jest ich stan sprzed skonfigurowania łączności.

Początkowa konfiguracja łączności

W tej sekcji opisano scenariusze konfiguracji łączności.

Konfigurowanie trybu Tylko chmura

Aby skonfigurować połączenie w trybie Tylko chmura

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Wybierz **Tylko chmura** i kliknij **Konfiguruj**.
   W wyniku tego w lokalizacji w chmurze zostanie wdrożona brama VPN i sieć w chmurze o zdefiniowanym adresie i masce.

Informacje na temat zarządzania sieciami w chmurze i konfigurowania ustawień bramy VPN można znaleźć w sekcji „Zarządzanie sieciami w chmurze”.

Konfigurowanie połączenia Open VPN site-to-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Wymagania urządzenia VPN

Wymagania systemowe

- 1 PROCESOR
- 1 GB PAMIĘCI RAM
- 8 GB miejsca na dysku

© Acronis International GmbH, 2003-2024

Porty

- TCP 443 (połączenia wychodzące) — do połączenia VPN
- TCP 80 (połączenia wychodzące) — do automatycznych aktualizacji urządzenia

Upewnij się, że zapory i inne składniki systemu zabezpieczeń sieci umożliwiają połączenia przez te porty z dowolnym adresem IP.

Konfigurowanie połączenia Open VPN site-to-site

Urządzenie VPN rozszerza Twoją sieć lokalną o chmurę przy użyciu bezpiecznego tunelu VPN. Połączenie tego rodzaju jest często nazywane połączeniem „site-to-site" (S2S). Możesz postąpić zgodnie z poniższą procedurą lub obejrzeć instruktaż wideo.

Aby skonfigurować połączenie za pośrednictwem urządzenia VPN

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Wybierz **Połączenie Open VPN site-to-site** i kliknij **Konfiguruj**.
   System rozpocznie wdrażanie bramy VPN w chmurze. Może to potrwać jakiś czas. W międzyczasie możesz przejść do następnego kroku.

   Uwaga
   Brama VPN jest udostępniana bez dodatkowych opłat. Zostanie usunięty w razie nieskorzystania z funkcji Disaster Recovery, tj. w razie braku jakiegokolwiek serwera podstawowego lub serwera odzyskiwania w chmurze przez 7 dni.

3. W sekcji **Urządzenie VPN** kliknij **Pobierz i wdróż**. Pobierz urządzenie VPN dla VMware vSphere lub Microsoft Hyper-V – zależnie od używanej platformy wirtualizacji.
4. Wdróż urządzenie i połącz je z sieciami produkcyjnymi.
   W środowisku vSphere upewnij się, że włączono **tryb nieograniczony** i że opcja **Fałszywe transmisje** ma ustawienie **Akceptuj** w przypadku wszystkich przełączników wirtualnych łączących urządzenie VPN z sieciami produkcyjnymi. Aby uzyskać dostęp do tych ustawień, wybierz w kliencie vSphere host > **Podsumowanie** > **Sieć** > przełącznik > **Edytuj ustawienia** > **Bezpieczeństwo**.
   Jeśli używasz Hyper-V, utwórz maszynę wirtualną typu **Generacja 1** mającą co najmniej 1024 MB pamięci. Warto też włączyć dla tej maszyny opcję **Pamięć dynamiczna**. Po utworzeniu maszyny kliknij **Ustawienia** > **Sprzęt** > **Karta sieciowa** > **Funkcje zaawansowane** i zaznacz pole wyboru obok opcji **Włącz fałszowanie adresów MAC**.
5. Włącz urządzenie
6. Przejdź do konsoli urządzenia i zaloguj się przy użyciu nazwy użytkownika i hasła „admin/admin".
7. [Opcjonalnie] Zmień hasło.
8. [Opcjonalnie] Zmień ustawienia sieci, jeśli jest to konieczne. Określ, który interfejs będzie używany jako interfejs sieci WAN na potrzeby połączenia z Internetem.

© Acronis International GmbH, 2003-2024

9. Zarejestruj urządzenie w usłudze Cyber Protection przy użyciu poświadczeń administratora firmy.
   Poświadczenia są używane tylko raz w celu pobrania certyfikatu. Adres URL centrum danych jest wstępnie zdefiniowany.

   Uwaga
   Jeśli na koncie jest skonfigurowane uwierzytelnianie dwuskładnikowe, pojawi się również monit o wprowadzenie kodu TOTP. Jeśli uwierzytelnianie dwuskładnikowe jest włączone, ale nie jest skonfigurowane na koncie, nie można zarejestrować urządzenia VPN. Najpierw trzeba przejść do strony logowania się do konsoli Cyber Protect i skonfigurować na koncie uwierzytelnianie dwuskładnikowe. Więcej informacji na temat uwierzytelniania dwuskładnikowego można znaleźć w Podręczniku administratora portalu zarządzania.

Gdy konfiguracja zostanie zakończona, urządzenie będzie miało status **Online**. Urządzenie połączy się z bramą VPN i zacznie zgłaszać usłudze Cyber Disaster Recovery Cloud informacje o sieciach ze wszystkich aktywnych interfejsów. Interfejsy te są wyświetlane w konsoli Cyber Protect na podstawie informacji z urządzenia VPN.

Konfigurowanie połączenia IPsec VPN multi-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Połączenie IPsec VPN multi-site można skonfigurować na dwa sposoby:

- Na karcie **Odzyskiwanie po awarii** > **Łączność**.
- Przez zastosowanie planu ochrony na jednym lub kilku urządzeniach, a następnie ręczne przełączenie z automatycznie utworzonego połączenia Open VPN site-to-site na połączenie IPsec VPN multi-site, skonfigurowanie ustawień IPsec VPN multi-site i zmianę przypisania adresów IP.

Aby skonfigurować połączenie IPsec VPN multi-site na karcie Łączność

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. W sekcji **Połączenie VPN multi-site** kliknij **Konfiguruj**.
   Brama VPN jest wdrażana w lokalizacji w chmurze.
3. Skonfiguruj ustawienia połączenia IPsec VPN multi-site.

Aby skonfigurować połączenie IPsec VPN multi-site w planie ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Zastosuj plan ochrony do jednego lub wielu urządzeń z listy.
   Serwer odzyskiwania i ustawienia infrastruktury chmury są automatycznie konfigurowane do łączności Open VPN site-to-site.
3. Wybierz **Odzyskiwanie po awarii** > **Łączność**.
4. Kliknij **Pokaż właściwości**.

© Acronis International GmbH, 2003-2024

5. Kliknij **Zmień na połączenie IPsec VPN multi-site**.
6. Skonfiguruj ustawienia połączenia IPsec VPN multi-site.
7. Zmień przypisanie adresów IP sieci w chmurze i serwerów chmurowych.

Konfigurowanie ustawień połączenia IPsec VPN multi-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Po skonfigurowaniu łączności IPsec VPN multi-site trzeba skonfigurować ustawienia lokalizacji w chmurze i lokalizacji lokalnych na karcie **Odzyskiwanie po awarii** > **Łączność**.

Wymagania wstępne

- Skonfigurowano łączność IPsec VPN multi-site. Dodatkowe informacje na temat konfigurowania łączności IPsec VPN multi-site można znaleźć w sekcji "Konfigurowanie połączenia IPsec VPN multi-site" (s. 810).
- Każda lokalna brama IPsec VPN ma publiczny adres IP.
- Dostępna sieć w chmurze ma wystarczająco dużo adresów IP dla serwerów chmurowych, które są kopiami chronionych komputerów (z sieci produkcyjnej), oraz dla serwerów odzyskiwania (z jednym lub dwoma adresami IP, w zależności od potrzeb).
- W przypadku stosowania zapory między lokalizacjami lokalnymi a lokalizacją w chmurze dozwolone są następujące protokoły IP i porty UDP w lokalizacjach lokalnych: Protokół IP ID 50 (ESP), port UDP 500 (IKE) i port UDP 4500.
- Konfiguracja NAT-T w miejscach lokalnych jest wyłączona.

Aby skonfigurować połączenie IPsec VPN multi-site

1. Dodaj jedną lub więcej sieci do lokalizacji w chmurze.
   a. Kliknij **Dodaj sieć**.

      Uwaga
      W przypadku dodawania sieci w chmurze odpowiednia sieć testowa jest dodawana automatycznie z tym samym adresem sieciowym i maską na potrzeby testowego przełączania awaryjnego. Serwery chmurowe w sieci testowej będą miały takie same adresy IP jak w sieci produkcyjnej w chmurze. Jeśli podczas testowego przełączenia awaryjnego jest konieczny dostęp do serwera chmurowego z sieci produkcyjnej, to w trakcie tworzenia serwera odzyskiwania należy przypisać drugi testowy adres IP.

   b. W polu **Adres sieciowy** wpisz adres IP sieci.

© Acronis International GmbH, 2003-2024

Uwaga
Upewnij się, że sieci w chmurze nie nakładają się na żadną sieć lokalną w środowisku. W przeciwnym razie nie będzie można ustanowić tunelu.

c. W polu **Maska sieci** wpisz adres maskę sieci.

d. Kliknij **Dodaj**.

2. Skonfiguruj ustawienia dla każdej lokalizacji lokalnej, która ma być połączona z lokalizacją w chmurze, zgodnie z zaleceniami dotyczącymi lokalizacji lokalnych. Dodatkowe informacje na temat tych zaleceń można znaleźć w sekcji "Ogólne zalecenia dotyczące lokalizacji lokalnych" (s. 813).

   a. Kliknij **Dodaj połączenie**.

   b. Wprowadź nazwę lokalnej bramy VPN.

   c. Wprowadź publiczny adres IP lokalnej bramy VPN.

   d. [Opcjonalnie] Wprowadź opis lokalnej bramy VPN.

   e. Kliknij **Dalej**.

   f. W polu **Klucz współdzielony (PSK)** wpisz klucz PSK lub kliknij **Wygeneruj nowy klucz współdzielony (PSK)**, aby użyć wartości wygenerowanej automatycznie.

   Uwaga
   W przypadku lokalnej i chmurowej bramy VPN trzeba użyć tego samego klucza PSK.

   g. Kliknij **Ustawienia zabezpieczeń IPsec/IKE**, aby skonfigurować te ustawienia. Dodatkowe informacje na temat ustawień, które można konfigurować, można znaleźć w sekcji "Ustawienia zabezpieczeń IPsec/IKE" (s. 813).

   Uwaga
   Można użyć ustawień domyślnych, które są wprowadzane automatycznie, lub użyć własnych wartości. Obsługiwane są tylko połączenia przy użyciu protokołu IKEv2. W przypadku ustanawiania łączności VPN domyślną wartością pola **Czynność podczas uruchamiania** jest **Dodaj** (połączenie inicjuje lokalna brama VPN), ale można ją zmienić na **Rozpocznij** (połączenie inicjuje chmurowa brama VPN) lub **Przekieruj** (opcja odpowiednia w przypadku zapór obsługujących opcję routingu).

   h. Skonfiguruj **Zasady dotyczące sieci**.
   Zasady dotyczące sieci określają, z którymi sieciami łączy się IPsec VPN. Wprowadź adres IP i maskę sieci w formacie CIDR. Segmenty sieci lokalnej i sieci w chmurze nie powinny się na siebie nakładać.

   i. Kliknij **Zapisz**.

© Acronis International GmbH, 2003-2024

Ogólne zalecenia dotyczące lokalizacji lokalnych

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Konfigurując lokalizacje lokalne pod kątem łączności IPsec VPN multi-site, warto wziąć pod uwagę następujące zalecenia:

- W przypadku każdej fazy IKE należy ustawić co najmniej jedną z wartości skonfigurowanych w lokalizacji w chmurze w ramach następujących parametrów: algorytm szyfrowania, algorytm skrótów i liczby z grup Diffiego-Hellmana.
- Włącz doskonałe utajnianie z wyprzedzeniem przy użyciu co najmniej jednej z wartości dla liczb z grup Diffiego-Hellmana skonfigurowanych w lokalizacji w chmurze w przypadku fazy 2 IKE.
- W przypadku fazy 1 IKE i fazy 2 IKE skonfiguruj tę samą wartość ustawienia **Czas aktywności** co w lokalizacji w chmurze.
- Konfiguracje z przechodzenie translacji NAT (NAT-T) nie są obsługiwane. Wyłącz konfigurację NAT-T w lokalizacji lokalnej. W przeciwnym razie nie będzie możliwa negocjacja dodatkowej hermetyzacji UDP.
- Konfiguracja **Czynność podczas uruchamiania** określa, która strona inicjuje połączenie. Wartość domyślna **Dodaj** oznacza, że lokalizacja lokalna inicjuje połączenie, a lokalizacja w chmurze oczekuje na zainicjowanie połączenia. Zmień wartość na **Rozpocznij**, jeśli to lokalizacja w chmurze ma inicjować połączenie, lub na **Przekieruj**, jeśli obie strony maja mieć możliwość inicjowania połączenia (ustawienie odpowiednie w przypadku zapór obsługujących opcję routingu).

Dodatkowe informacje i przykłady konfiguracji dotyczące innych rozwiązań można znaleźć na stronie:

- Seria artykułów z bazy wiedzy Knowledge Base
- Film z przykładem

Ustawienia zabezpieczeń IPsec/IKE

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Poniższa tabela zawiera dodatkowe informacje na temat parametrów zabezpieczeń IPsec/IKE.

Parametr	Opis
Algorytm szyfrowania	Algorytm szyfrowania, który będzie używany do blokowania wglądu w dane podczas przesyłania. Domyślnie są wybrane wszystkie algorytmy. Na lokalnym urządzeniu bramy trzeba skonfigurować co najmniej jeden z wybranych algorytmów dla

© Acronis International GmbH, 2003-2024

Parametr	Opis
	każdej fazy IKE.
Algorytm skrótów	Algorytm skrótów, który będzie używany do weryfikowania integralności i autentyczności danych. Domyślnie są wybrane wszystkie algorytmy. Na lokalnym urządzeniu bramy trzeba skonfigurować co najmniej jeden z wybranych algorytmów dla każdej fazy IKE.
Liczby z grup Diffiego-Hellmana	Liczby z grup Diffiego-Hellmana definiują siłę klucza używanego w procesie wymiany kluczy Internet Key Exchange (IKE). Liczby z wyższych grup są bezpieczniejsze, ale wymagają dodatkowego czasu na obliczenie klucza. Domyślnie są wybrane wszystkie grupy. Na lokalnym urządzeniu bramy trzeba skonfigurować co najmniej jedną z wybranych grup dla każdej fazy IKE.
Czas aktywności (w sekundach)	Wartość czasu aktywności oznacza czas trwania instancji połączenia z ustawionymi kluczami szyfrowania/uwierzytelniania dla pakietów użytkowników: od pomyślnej negocjacji po wygaśnięcie. Zakres dla fazy 1: 900–28800 s, domyślny: 28800. Zakres dla fazy 2: 900–3600 s, domyślny: 3600. Czas aktywności dla fazy 2 musi być krótszy od czasu aktywności dla fazy 1. Połączenie jest ponownie negocjowane przez kanał negocjujący klucz przed jego wygaśnięciem. Zobacz **Czas marginesu ponownej negocjacji klucza**. Jeśli strona lokalna i zdalna nie zgadzają się co do czasu aktywności, po stronie z dłuższym czasem aktywności wystąpią bezładne zastąpione połączenia. Zobacz także **Czas marginesu ponownej negocjacji klucza** i **Zakres wahań ponownej negocjacji kluczy**.
Czas marginesu ponownej negocjacji klucza (w sekundach)	Czas marginesu poprzedzający wygaśnięcie połączenia lub kanału negocjacji klucza, w ramach którego lokalna strona połączenia VPN próbuje wynegocjować zamianę. Dokładny czas ponownej negocjacji klucza jest wybierany losowo z

© Acronis International GmbH, 2003-2024

Parametr	Opis
	uwzględnieniem wartości **Zakres wahań ponownej negocjacji kluczy**. Jest to istotne tylko lokalnie — strona zdalna nie musi się na to zgadzać. Zakres: 900–3600 s. Wartość domyślna to 3600.
Rozmiar okna tłumienia ataku powtórki (pakiet)	Rozmiar okna tłumienia ataku powtórki dla połączenia. Domyślna wartość -1 używa wartości skonfigurowanej za pomocą charon.replay_window w pliku strongswan.conf. Wartości większe niż 32 są obsługiwane tylko w przypadku korzystania z infrastruktury zaplecza Netlink. Wartość 0 powoduje wyłączenie ochronę IPsec przed atakami powtórki.
Zakres wahań ponownej negocjacji kluczy (%)	Maksymalny procent, o jaki losowo są zwiększane wartości bajtów, pakietów i czasu marginesu w celu randomizacji przedziałów czasu ponownej negocjacji kluczy (istotne w przypadku hostów z wieloma połączeniami). Wartość zakresu wahań ponownej negocjacji kluczy może przekraczać 100%. Wartość ustawienia marginTYPE po losowym zwiększeniu nie może przekraczać progu lifeTYPE, gdzie TYPE jest jednym z bajtów bądź pakietów albo czasem. Wartość 0% powoduje wyłączenie randomizacji. Jest to istotne tylko lokalnie — strona zdalna nie musi się na to zgadzać.
Limit czasu funkcji DPD (w sekundach)	Czas, po którym następuje upłynięcie limitu czasu funkcji Dead Peer Detection (DPD). Można określić wartość 30 lub wyższą. Wartość domyślna to 30.
Czynność po upłynięciu limitu czasu funkcji Dead Peer Detection (DPD)	Czynność podejmowana po upłynięciu limitu czasu funkcji Dead Peer Detection (DPD). **Uruchom ponownie** — po upłynięciu limitu czasu funkcji DPD nastąpi ponowne uruchomienie sesji. **Wyczyść** — po upłynięciu limitu czasu funkcji DPD nastąpi zakończenie sesji. **Brak** — po upłynięciu limitu czasu funkcji DPD nie zostanie podjęta żadna czynność.

© Acronis International GmbH, 2003-2024

Parametr	Opis
Czynność podczas uruchamiania	Określa, która strona inicjuje połączenie i ustanawia tunel dla połączenia VPN. **Dodaj** — połączenie inicjuje lokalna brama VPN. **Rozpocznij** — połączenie inicjuje brama VPN w chmurze. **Przekieruj** — opcja odpowiednia w przypadku bram VPN obsługujących opcję routingu. tunel jest aktywny tylko wtedy, gdy ruch jest inicjowany z lokalnej bramy VPN lub chmurowej bramy VPN.

Zalecenia dotyczące dostępności usług Active Directory Domain Services

Jeśli chronione obciążenia muszą być uwierzytelniane na kontrolerze domeny, zalecamy zastosowanie instancji kontrolera domeny usługi Active Directory w lokalizacji usługi Disaster Recovery.

Kontroler domeny usługi Active Directory na potrzeby łączności L2 Open VPN

Dzięki łączności L2 Open VPN adresy IP chronionych obciążeń są zachowywane w lokalizacji w chmurze podczas testowego lub produkcyjnego przełączania awaryjnego. W związku z tym kontroler domeny usługi Active Directory podczas testowego lub produkcyjnego przełączania awaryjnego ma taki sam adres IP jak w lokalizacji lokalnej.

Dzięki niestandardowym ustawieniom usługi DNS możesz ustawić własny serwer DNS dla wszystkich serwerów chmurowych. Aby uzyskać więcej informacji, zobacz "Konfigurowanie niestandardowych serwerów DNS" (s. 826).

Kontroler domeny usługi Active Directory na potrzeby łączności L3 IPsec VPN

W przypadku łączności L3 IPsec VPN adresy IP chronionych obciążeń nie są zachowywane w lokalizacji w chmurze. Dlatego przed wykonaniem produkcyjnego przełączenia awaryjnego warto wdrożyć dodatkową specjalną instancję kontrolera domeny usługi AD jako serwer podstawowy w lokalizacji w chmurze.

Oto zalecenia dotyczące specjalnej instancji kontrolera domeny usługi AD skonfigurowanej jako serwer podstawowy w lokalizacji w chmurze:

- Wyłącz Zaporę systemu Windows.
- Dołącz serwer podstawowy do usługi Active Directory.
- Dopilnuj, aby serwer podstawowy miał dostęp do Internetu.
- Dodaj funkcję Active Directory.

© Acronis International GmbH, 2003-2024

Dzięki niestandardowym ustawieniom usługi DNS możesz ustawić własny serwer DNS dla wszystkich serwerów chmurowych. Aby uzyskać więcej informacji, zobacz "Konfigurowanie niestandardowych serwerów DNS" (s. 826).

Konfigurowanie zdalnego dostępu VPN point-to-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W przypadku konieczności nawiązania połączenia zdalnego z lokalizacją lokalną można skonfigurować połączenie point-to-site z lokalizacją lokalną. Możesz postąpić zgodnie z poniższą procedurą lub obejrzeć instruktaż wideo.

Wymagania wstępne

- Skonfigurowano połączenie Open VPN site-to-site.
- Urządzenie VPN jest zainstalowane w lokalizacji lokalnej.

Aby skonfigurować połączenie point-to-site z lokalizacją lokalną

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Włącz opcję **Dostęp VPN do lokalizacji lokalnej**.
4. Sprawdź, czy użytkownik nawiązujący połączenie point-to-site z lokalizacją lokalną ma:
   - Konto użytkownika na platformie Cyber Protect Cloud. To tych poświadczeń musi użyć w celu uwierzytelnienia się w kliencie VPN. Jeśli nie ma, utwórz odpowiednie konto użytkownika na platformie Cyber Protect Cloud.
   - Rolę użytkownika „Administrator firmy” lub „Cyber Protection”.
5. Skonfiguruj klienta OpenVPN:
   a. Pobierz klienta OpenVPN w wersji 2.4.0 lub nowszej ze strony: https://openvpn.net/community-downloads/.

      Uwaga
      Klient OpenVPN Connect nie jest obsługiwany.

   b. Zainstaluj klienta OpenVPN na komputerze, z którego chcesz się połączyć z lokalizacją lokalną.
   c. Kliknij **Pobierz konfigurację dla pakietu OpenVPN**. Plik konfiguracyjny działa w przypadku użytkowników z organizacji mających rolę użytkownika „Administrator firmy” lub „Cyberochrona”.
   d. Zaimportuj pobraną konfigurację do klienta OpenVPN.
   e. Zaloguj się do klienta OpenVPN, korzystając ze swoich poświadczeń użytkownika z platformy Cyber Protect Cloud (patrz krok 4 powyżej).

© Acronis International GmbH, 2003-2024

f. [Opcjonalnie] Jeśli w organizacji jest włączone uwierzytelnianie dwuskładnikowe, podaj również wygenerowany jednorazowy kod TOTP.

Ważne
W przypadku włączenia dla konta uwierzytelniania dwuskładnikowego trzeba ponownie wygenerować plik konfiguracyjny i odnowić go na potrzeby istniejących klientów OpenVPN. Aby skonfigurować uwierzytelnianie dwuskładnikowe dla swojego konta, użytkownik musi się ponownie zalogować na platformie Cyber Protect Cloud.

Dzięki temu będzie można nawiązywać połączenia z komputerami w lokalizacji lokalnej.

Zarządzanie sieciami

W tej sekcji opisano scenariusze zarządzania sieciami.

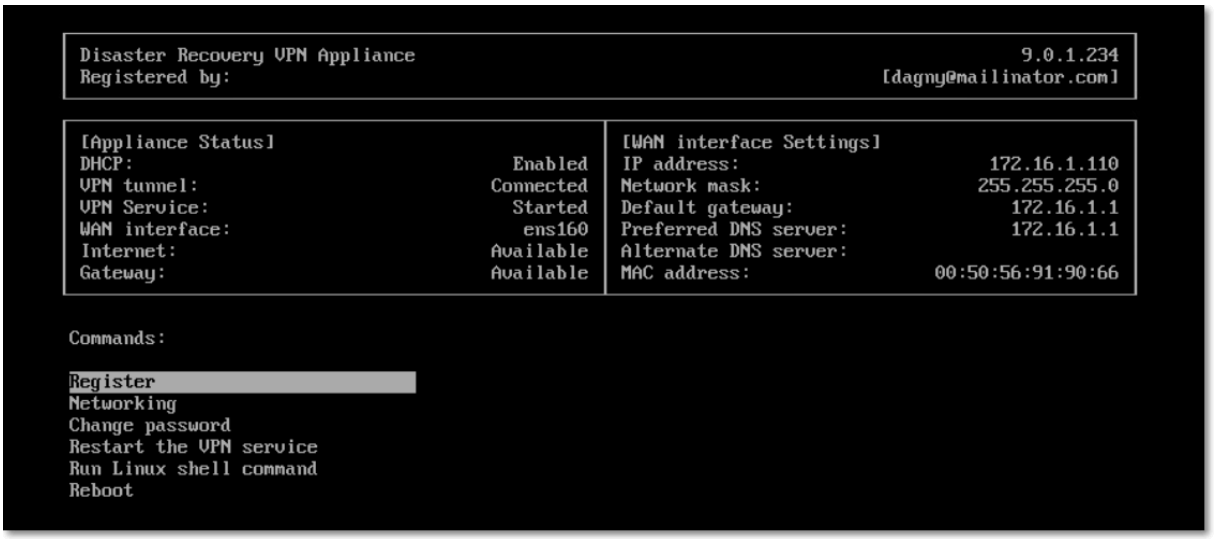
Zarządzanie sieciami

Uwaga
Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Połączenie Open VPN site-to-site

Aby dodać sieć do lokalizacji lokalnej i rozszerzyć ją o chmurę

1. Skonfiguruj w urządzeniu VPN nowy interfejs sieciowy dla sieci lokalnej, którą chcesz rozszerzyć o chmurę.
2. Zaloguj się do konsoli urządzenia VPN.
3. W sekcji **Sieć** skonfiguruj ustawienia sieciowe nowego interfejsu.



© Acronis International GmbH, 2003-2024

Urządzenie VPN zacznie zgłaszać usłudze Cyber Disaster Recovery Cloud informacje o sieciach ze wszystkich aktywnych interfejsów. Interfejsy te są wyświetlane w konsoli Cyber Protect na podstawie informacji z urządzenia VPN.

Aby usunąć sieć rozszerzoną o chmurę

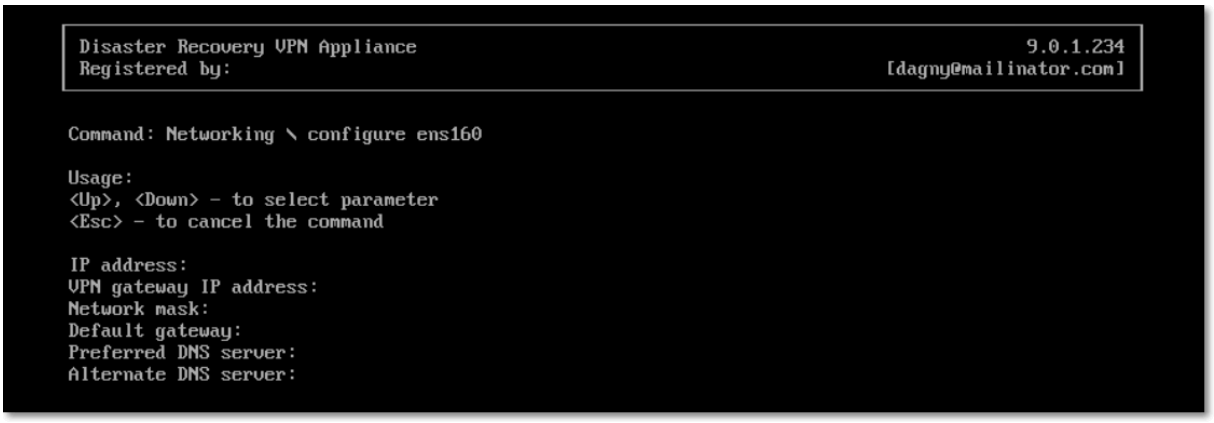
1. Zaloguj się do konsoli urządzenia VPN.
2. W sekcji **Sieć** wybierz interfejs, który chcesz usunąć, a następnie kliknij **Wyczyść ustawienia sieciowe**.
3. Potwierdź operację.

W rezultacie zostanie wyłączone rozszerzenie sieci lokalnej o chmurę przy użyciu bezpiecznego tunelu VPN. Sieć będzie działać jako niezależny segment chmury. Jeśli ten interfejs służył do przekazywania ruchu z (do) lokalizacji w chmurze, wszystkie połączenia sieciowe z (do) lokalizacji w chmurze zostaną zerwane.

Aby zmienić parametry sieciowe

1. Zaloguj się do konsoli urządzenia VPN.
2. W sekcji **Sieć** wybierz interfejs, który chcesz edytować.
3. Kliknij **Edytuj ustawienia sieciowe**.
4. Wybierz jedną z dwóch możliwych opcji:
   - Aby uzyskać automatyczną konfigurację sieci przez DHCP, kliknij **Użyj DHCP**. Potwierdź operację.
   - Aby ręcznie skonfigurować sieć, kliknij **Ustaw statyczny adres IP**. Można edytować następujące ustawienia:
     - **Adres IP** — adres IP interfejsu w sieci lokalnej.
     - **Adres IP bramy VPN** — specjalny adres IP zarezerwowany dla tego chmurowego segmentu sieci w celu zapewnienia odpowiedniego działania usługi Cyber Disaster Recovery Cloud.
     - **Maska sieci** — maska sieci lokalnej.
     - **Brama domyślna** — domyślna brama w lokalizacji lokalnej.
     - **Preferowany serwer DNS** — podstawowy serwer DNS w lokalizacji lokalnej.
     - **Alternatywny serwer DNS** — dodatkowy serwer DNS w lokalizacji lokalnej.

© Acronis International GmbH, 2003-2024



- Wprowadź niezbędne zmiany i potwierdź je klawiszem Enter.

Tryb Tylko chmura

W chmurze można mieć do 23 sieci.

Aby dodać nową sieć w chmurze

1. Wybierz **Odzyskiwanie po awarii** > **Łączność**.
2. W sekcji **Lokalizacja w chmurze** kliknij **Dodaj sieć w chmurze**.
3. Zdefiniuj parametry sieci w chmurze: adres i maskę sieci. Gdy skończysz, kliknij **Gotowe**.

W rezultacie do lokalizacji w chmurze zostanie dodana sieć o zdefiniowanym adresie i masce.

Aby usunąć sieć w chmurze

Uwaga
Jeśli w sieci w chmurze znajduje się choć jeden serwer chmurowy, nie można jej usunąć. Najpierw trzeba usunąć serwer chmurowy, a dopiero potem sieć.

1. Wybierz **Odzyskiwanie po awarii** > **Łączność**.
2. Na karcie **Lokalizacja w chmurze** kliknij adres sieci, którą chcesz usunąć.
3. Kliknij **Usuń** i potwierdź operację.

Aby zmienić parametry sieci w chmurze

1. Wybierz **Odzyskiwanie po awarii** > **Łączność**.
2. Na karcie **Lokalizacja w chmurze** kliknij adres sieci, którą chcesz edytować.
3. Kliknij **Edytuj**.
4. Zdefiniuj adres oraz maskę sieci i kliknij **Gotowe**.

Zmienianie konfiguracji adresu IP

Aby uzyskać właściwą wydajność odzyskiwania po awarii, trzeba zadbać o spójność adresów IP przypisanych do serwerów lokalnych i chmurowych. W razie jakichkolwiek niespójności lub

© Acronis International GmbH, 2003-2024

niedopasowania adresów IP obok odpowiadającej adresowi sieci na stronie **Odzyskiwanie po awarii** > **Łączność** będzie wyświetlany wykrzyknik.

Poniżej przedstawiono kilka powszechnie znanych przyczyn niespójności adresów IP:

1. Przeniesiono serwer odzyskiwania z jednej sieci do drugiej lub zmieniono maskę sieci w chmurze. W rezultacie serwery chmurowe mają adresy IP z sieci, do których nie są podłączone.
2. Zmieniono typ łączności z „Bez połączenia site-to-site" na „Połączenie site-to-site". W rezultacie serwer lokalny znajduje się w innej sieci niż ta, która została utworzona dla serwera odzyskiwania w lokalizacji w chmurze.
3. Zmieniono typ łączności z Open VPN site-to-site na IPsec VPN multi-site lub z IPsec VPN multi-site na Open VPN site-to-site. Dodatkowe informacje na temat tego scenariusza można znaleźć w sekcjach Zmienianie połączeń i Zmienianie przypisania adresów IP.
4. Edytowano następujące parametry sieciowe na stronie urządzenia VPN:
   - Dodano interfejs przez ustawienia sieciowe
   - Ręcznie edytowano maskę sieci przez ustawienia interfejsu
   - Edytowano maskę sieci przez DHCP
   - Ręcznie edytowano adres i maskę sieci przez ustawienia interfejsu
   - Edytowano maskę i adres sieci przez DHCP

   W wyniku wymienionych wyżej działań sieć w lokalizacji w chmurze może stać się obszarem podrzędnym lub nadrzędnym sieci lokalnej albo interfejs urządzenia VPN może zgłosić te same ustawienia sieciowe w przypadku różnych interfejsów.

Aby rozwiązać problem z ustawieniami sieciowymi

1. Kliknij sieć wymagającą zmiany konfiguracji adresu IP.
   Zostanie wyświetlona lista serwerów znajdujących się w wybranej sieci, ich statusów i adresów IP. Serwery o niespójnych ustawieniach sieciowych są oznaczone wykrzyknikiem.
2. Aby zmienić ustawienia sieciowe serwera, kliknij **Przejdź do serwera**. Aby zmienić ustawienia sieciowe wszystkich serwerów naraz, kliknij **Zmień** w obszarze powiadomień.
3. Zmień adresy IP stosownie do potrzeb, definiując je w polach **Nowy adres IP** i **Nowy testowy adres IP**.
4. Gdy skończysz, kliknij **Potwierdź**.

Przenoszenie serwerów do odpowiedniej sieci

Po utworzeniu planu ochrony na potrzeby odzyskiwania po awarii i zastosowaniu go do wybranych urządzeń system sprawdza adresy IP urządzeń i automatycznie tworzy sieci w chmurze, jeśli nie ma jeszcze sieci w chmurze, do których pasuje adres IP. Domyślnie sieci w chmurze są konfigurowane z maksymalnymi zakresami zalecanymi przez IANA do użytku prywatnego (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Sieć można zawęzić, edytując jej maskę.

Jeśli wybrane urządzenia znajdują się w wielu sieciach lokalnych, sieć w chmurze może stać się obszarem nadrzędnym w stosunku do tych sieci lokalnych. W takim przypadku można zmienić konfigurację sieci w chmurze:

© Acronis International GmbH, 2003-2024

1. Kliknij sieć w chmurze wymagającą zmiany konfiguracji rozmiaru sieci i kliknij **Edytuj**.
2. Skonfiguruj ponownie rozmiar sieci przy użyciu poprawnych ustawień.
3. Utwórz inne wymagane sieci.
4. Kliknij ikonę powiadomienia obok liczby urządzeń podłączonych do sieci.
5. Kliknij **Przenieś do odpowiedniej sieci**.
6. Zaznacz serwery, które chcesz przenieść do odpowiednich sieci, a następnie kliknij **Przenieś**.

Zarządzanie ustawieniami urządzenia VPN

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W konsoli Cyber Protect (**Odzyskiwanie po awarii** > **Łączność**) można:

- Pobrać pliki dzienników.
- Wyrejestrować urządzenie (jeśli trzeba zresetować ustawienia urządzenia VPN lub zmienić tryb na Tylko chmura).

Aby uzyskać dostęp do tych ustawień, kliknij ikonę **i** w sekcji **Urządzenie VPN**.

W konsoli urządzenia VPN można:

- Zmienić hasło urządzenia.
- Wyświetlić/zmienić ustawienia sieciowe i określić, który interfejs ma być używany jako interfejs sieci WAN na potrzeby połączenia z Internetem.
- Zarejestrować lub zmienić zarejestrowane konto (drogą ponownej rejestracji).
- Uruchomić ponownie usługę VPN.
- Zrestartować urządzenie VPN.
- Uruchomić polecenie powłoki systemu Linux (tylko w przypadku zaawansowanego rozwiązywania problemu).

Ponowne instalowanie bramy VPN

W razie napotkania problemu z bramą VPN, którego nie uda się rozwiązać, może być konieczna ponowna instalacja bramy VPN. Możliwe są między innymi następujące problemy:

- Brama VPN ma status **Błąd**.
- Brama VPN przez długi czas ma status **Oczekujące**.
- Od dłuższego czasu nie ustalono statusu bramy VPN.

Proces ponownej instalacji bramy VPN obejmuje następujące zautomatyzowane czynności: całkowite usunięcie obecnej maszyny wirtualnej z bramą VPN, zainstalowanie nowej maszyny

© Acronis International GmbH, 2003-2024

wirtualnej z szablonu oraz zastosowanie ustawień poprzedniej bramy VPN na nowej maszynie wirtualnej.

Wymagania wstępne:

Trzeba ustawić typ łączności z lokalizacją w chmurze.

Aby ponownie zainstalować bramę VPN

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij ikonę koła zębatego obok bramy VPN i wybierz **Zainstaluj ponownie bramę VPN**.
3. W oknie dialogowym **Zainstaluj ponownie bramę VPN** wprowadź swoją nazwę logowania.
4. Kliknij **Zainstaluj ponownie**.

Włączanie i wyłączanie połączenia site-to-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Połączenie site-to-site warto włączyć w następujących przypadkach:

- Jeśli serwery chmurowe z lokalizacji w chmurze muszą się komunikować z serwerami w lokalizacji lokalnej.
- Po przełączeniu awaryjnym na chmurę przywrócono normalne działanie lokalnej infrastruktury i chcesz przywrócić serwery do lokalizacji lokalnej przy użyciu operacji powrotu po awarii.

Aby włączyć połączenie site-to-site

1. Wybierz **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij **Pokaż właściwości** i włącz opcję **Połączenie site-to-site**.

W wyniku tego zostanie aktywowane połączenie VPN site-to-site między lokalizacją lokalną i lokalizacją w chmurze. Usługa Cyber Disaster Recovery Cloud uzyskuje ustawienia sieciowe z urządzenia VPN i rozszerza sieci lokalne o lokalizację w chmurze.

Jeśli serwery chmurowe z lokalizacji w chmurze nie muszą się komunikować z serwerami w lokalizacji lokalnej, można wyłączyć połączenie site-to-site.

Aby wyłączyć połączenie site-to-site

1. Wybierz **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij **Pokaż właściwości** i wyłącz opcję **Połączenie site-to-site**.

W rezultacie lokalizacja lokalna zostanie odłączona od lokalizacji w chmurze.

© Acronis International GmbH, 2003-2024

Zmienianie typu łączności na site-to-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Typ łączności można łatwo zmienić z Open VPN site-to-site na IPsec VPN multi-site oraz z IPsec VPN multi-site na Open VPN site-to-site.

Po zmianie typu łączności aktywne połączenia VPN są usuwane, ale konfiguracje serwerów chmurowych i sieci zostają zachowane. Nadal jednak trzeba będzie zmienić przypisanie adresów IP sieci i serwerów w chmurze.

W poniższej tabeli zamieszczono porównanie podstawowych cech połączenia Open VPN site-to-site i połączenia IPsec VPN multi-site.

	Połączenie Open VPN site-to-site	**Połączenia IPsec VPN multi-site**
Obsługa lokalizacji lokalnych	Jedna	Jedna, wiele
Tryb bramy VPN	L2 Open VPN	L3 IPsec VPN
Segmenty sieci	Rozszerzenie sieci lokalnej na sieć w chmurze	Segmenty sieci lokalnej i sieci w chmurze nie powinny się na siebie nakładać.
Obsługa dostępu point-to-site do lokalizacji lokalnej	Tak	Nie
Obsługa dostępu point-to-site do lokalizacji w chmurze	Tak	Tak
Wymóg pozycji oferty publicznego adresu IP	Nie	Tak

Aby zmienić połączenie Open VPN site-to-site na połączenie IPsec VPN multi-site

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Zmień na połączenie IPsec VPN multi-site**.
4. Kliknij **Zmień konfigurację**.
5. Zmień przypisanie adresów IP sieci w chmurze i serwerów chmurowych.
6. Skonfiguruj ustawienia połączenia IPsec multi-site.

Aby zmienić połączenie IPsec VPN multi-site na połączenie Open VPN site-to-site

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Zmień na połączenie Open VPN site-to-site**.
4. Kliknij **Zmień konfigurację**.
5. Zmień przypisanie adresów IP sieci w chmurze i serwerów chmurowych.
6. Skonfiguruj ustawienia połączenia site-to-site.

Zmienianie przypisania adresów IP

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W następujących przypadkach w celu ukończenia konfiguracji trzeba zmienić przypisanie adresów IP do sieci i serwerów chmurowych:

- Zmieniono typ łączności z Open VPN site-to-site na IPsec VPN multi-site lub na odwrót.
- Zastosowano plan ochrony (jeśli jest skonfigurowana łączność IPsec VPN multi-site).

Aby zmienić przypisanie adresu IP sieci w chmurze

1. Na karcie **Łączność** kliknij adres IP sieci w chmurze.
2. W wyskakującym okienku **Sieć** kliknij **Edytuj**.
3. Wprowadź nowy adres i maskę sieci.
4. Kliknij **Gotowe**.

Po zmianie przypisania adresu IP sieci w chmurze należy zmienić przypisanie serwerów chmurowych znajdujących się w tej sieci.

Aby zmienić przypisanie adresu IP serwera

1. Na karcie **Łączność** kliknij adres IP serwera w danej sieci w chmurze.
2. W wyskakującym okienku **Serwery** kliknij **Zmień adres IP**.
3. W wyskakującym okienku **Zmień adres IP** wpisz nowy adres IP serwera lub użyj automatycznie wygenerowanego adresu IP należącego do sieci w chmurze, której przypisanie zmieniono.

   Uwaga
   Usługa Cyber Disaster Recovery Cloud automatycznie przypisuje adresy IP z sieci w chmurze do wszystkich serwerów chmurowych należących do tej sieci przed zmianą przypisania jej adresu IP. Sugerowane adresy IP można wykorzystać do zmiany przypisania adresów IP wszystkich serwerów chmurowych naraz.

4. Kliknij **Potwierdź**.

© Acronis International GmbH, 2003-2024

Konfigurowanie niestandardowych serwerów DNS

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Podczas konfigurowania łączności usługa Cyber Disaster Recovery Cloud tworzy infrastrukturę sieci w chmurze. Serwer DHCP w chmurze automatycznie przypisuje domyślne serwery DNS do serwerów odzyskiwania i serwerów podstawowych, ale można zmienić ustawienia domyślne i skonfigurować niestandardowe serwery DNS. Nowe ustawienia serwerów DNS zostaną zastosowane od następnego żądania skierowanego do serwera DHCP.

Wymagania wstępne:

Trzeba ustawić typ łączności z lokalizacją w chmurze.

Aby skonfigurować niestandardowy serwer DNS

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Domyślne (dostępne w lokalizacji w chmurze)**.
4. Wybierz **Serwery niestandardowe**.
5. Wpisz adres IP serwera DNS.
6. [Opcjonalnie] Jeśli chcesz dodać kolejny serwer DNS, kliknij **Dodaj** i wpisz adres IP tego serwera DNS.

   Uwaga
   Po dodaniu niestandardowych serwerów DNS możesz też dodać domyślne serwery DNS. Dzięki temu w przypadku niedostępności niestandardowych serwerów DNS usługa Cyber Disaster Recovery Cloud skorzysta z domyślnego serwera DNS.

7. Kliknij **Gotowe**.

Usuwanie niestandardowych serwerów DNS

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Można usuwać serwery DNS z listy niestandardowych serwerów DNS.

Wymagania wstępne:

Skonfigurowano niestandardowe serwery DNS.

© Acronis International GmbH, 2003-2024

Aby usunąć niestandardowy serwer DNS

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Serwery niestandardowe**.
4. Kliknij ikonę usuwania obok nazwy serwera DNS.

   Uwaga
   Jeśli jest dostępny tylko jeden niestandardowy serwer DNS, operacja usuwania jest wyłączona. Jeśli chcesz usunąć wszystkie niestandardowe serwery DNS, wybierz **Domyślne (dostępne w lokalizacji w chmurze)**.

5. Kliknij **Gotowe**.

Konfigurowanie routingu lokalnego

Oprócz sieci lokalnych, które są rozszerzane o chmurę za pomocą urządzenia VPN, można mieć inne sieci lokalne, które nie są zarejestrowane w urządzeniu VPN, ale znajdujące się w nich serwery muszą się komunikować z serwerami chmurowymi. Aby zapewnić łączność między takimi serwerami lokalnymi a serwerami chmurowymi, należy skonfigurować ustawienia routingu lokalnego.

Aby skonfigurować routing lokalny

1. Przejdź do karty **Odzyskiwanie po awarii** >**Łączność**.
2. Kliknij **Pokaż właściwości**, a następnie **Routing lokalny**.
3. Wskaż sieci lokalne w notacji CIDR.
4. Kliknij **Zapisz**.

W wyniku tych działań serwery z określonych sieci lokalnych mogą się komunikować z serwerami chmurowymi.

Zezwalanie na ruch DHCP przez połączenie L2 VPN

Jeśli urządzenia w lokalizacji lokalnej uzyskują adresy IP z serwera DHCP, można chronić ten serwer DHCP za pomocą funkcji Odzyskiwanie po awarii, przełączyć go awaryjnie do chmury, a następnie zezwolić na ruch DHCP przez połączenie L2 VPN. W wyniku tych czynności serwer DHCP będzie działać w chmurze, ale nadal będzie przydzielać adresy IP urządzeniom lokalnym.

Wymagania wstępne:

Trzeba ustawić łączność L2 VPN site-to-site z lokalizacją w chmurze.

Aby zezwolić na ruch DHCP przez połączenie L2 VPN

1. Przejdź do karty **Odzyskiwanie po awarii** >**Łączność**.
2. Kliknij **Pokaż właściwości**.

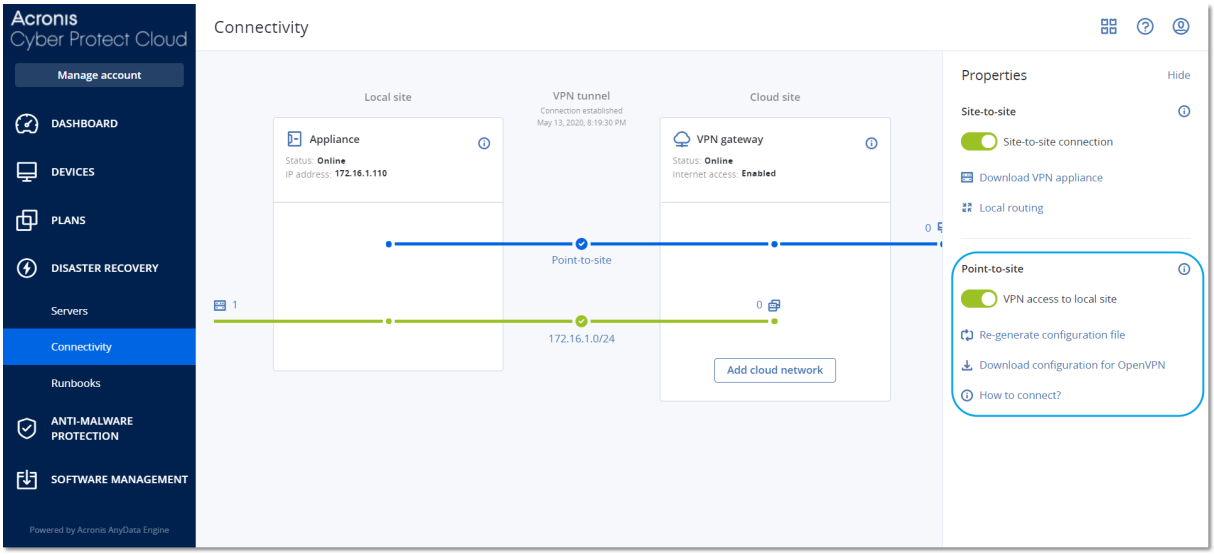
© Acronis International GmbH, 2003-2024

3. Włącz przełącznik **Zezwól na ruch DHCP przez połączenie L2 VPN**.

Zarządzanie ustawieniami połączenia point-to-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność** i kliknij **Pokaż właściwości** w prawym górnym rogu okna.



Dostęp VPN do lokalizacji lokalnej

Ta opcja służy do zarządzania dostępem VPN do lokalizacji lokalnej. Domyślnie jest ona włączona. W przypadku jej wyłączenia dostęp point-to-site do lokalizacji lokalnej nie będzie dozwolony.

Pobierz konfigurację dla pakietu OpenVPN

Spowoduje to pobranie pliku konfiguracji klienta OpenVPN. Plik ten jest wymagany do nawiązania połączenia point-to-site z lokalizacją w chmurze.

Ponowne generowanie konfiguracji

Możesz ponownie wygenerować plik konfiguracyjny klienta OpenVPN.

Jest to wymagane w następujących przypadkach:

- Jeśli podejrzewasz, że do pliku konfiguracyjnego mogły mieć dostęp osoby niepowołane.
- Jeśli na Twoim koncie włączono uwierzytelnianie dwuskładnikowe.

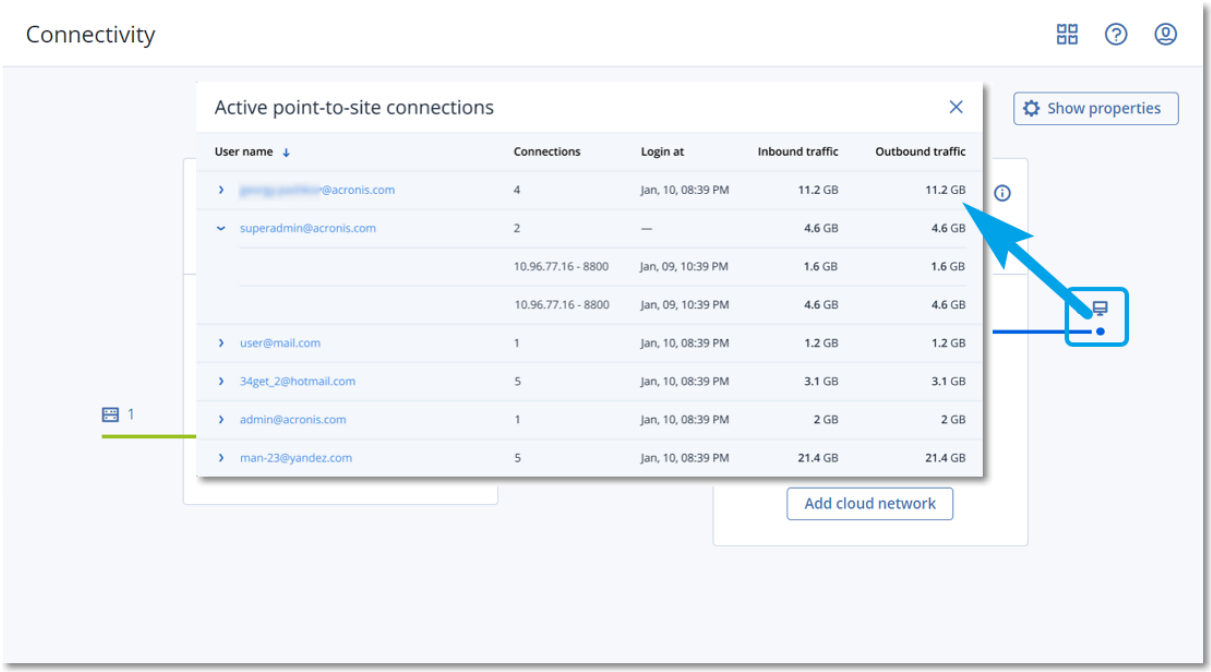
Po zaktualizowaniu pliku konfiguracyjnego nie można nawiązać połączenia przy użyciu starego pliku. Udostępnij nowy plik konfiguracyjny wszystkim użytkownikom uprawnionym do korzystania z połączenia point-to-site.

© Acronis International GmbH, 2003-2024

Aktywne połączenia point-to-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Wszystkie aktywne połączenia point-to-site można zobaczyć w sekcji **Odzyskiwanie po awarii** > **Łączność**. Kliknij ikonę komputera na niebieskiej linii **Point-to-site** — zostaną wyświetlone szczegółowe informacje o aktywnych połączeniach point-to-site pogrupowanych według nazwy użytkownika.



Praca z dziennikami

Funkcja Odzyskiwanie po awarii zbiera dzienniki w przypadku urządzenia VPN i bramy VPN. Dzienniki są zapisywane w postaci plików .txt i kompresowane w archiwum .zip. Możesz pobrać i wyodrębnić archiwum, a następnie skorzystać z tych informacji w celu rozwiązania problemów lub monitorowania.

Poniższa lista udostępnia opisy plików dzienników zawartych w archiwum .zip oraz zawartych w nich informacji.

`dnsmasq.config.txt` — ten plik zawiera informacje o konfiguracji usługi udostępniającej adresy DNS i DHCP.

`dnsmasq.leases.txt` — ten plik zawiera informacje o bieżących dzierżawach adresów DHCP.

`dnsmasq_log.txt` — ten plik zawiera dzienniki usługi dnsmasq.

`ebtables.txt` — ten plik zawiera informacje o tabelach zapory.

`free.txt` — ten plik zawiera informacje o wolnym miejscu w pamięci.

© Acronis International GmbH, 2003-2024

`ip.txt` — ten plik zawiera dzienniki z konfiguracji interfejsów sieciowych, w tym ich nazwy, które można wykorzystać w konfiguracji ustawień funkcji **Przechwytywanie pakietów sieciowych**.

`NetworkManager_log.txt` — ten plik zawiera dzienniki z usługi NetworkManager.

`NetworkManager_status.txt` — ten plik zawiera informacje o statusie usługi NetworkManager.

`openvpn@p2s_log.txt` — ten plik zawiera dzienniki z usługi OpenVPN.

`openvpn@p2s_status.txt` — ten plik zawiera informacje o statusie tuneli VPN.

`ps.txt` — ten plik zawiera informacje o aktualnie uruchomionych procesach na bramie VPN lub urządzeniu VPN.

`resolf.conf.txt` — ten plik zawiera informacje o konfiguracji serwerów DNS.

`routes.txt` — ten plik zawiera informacje o trasach sieciowych.

`uname.txt` — ten plik zawiera informacje o bieżącej wersji jądra systemu operacyjnego.

`uptime.txt` — ten plik zawiera informacje o czasie, przez jaki system operacyjny nie był ponownie uruchamiany.

`vpnserver_log.txt` — ten plik zawiera dzienniki z usługi VPN.

`vpnserver_status.txt` — ten plik zawiera informacje o statusie serwera VPN.

Dodatkowe informacje na temat plików dzienników dotyczących łączności IPsec VPN można znaleźć w sekcji "Pliki dziennika IPsec VPN multi-site" (s. 834).

Pobieranie dzienników urządzenia VPN

Możesz pobrać i wyodrębnić archiwum zawierające dzienniki urządzenia VPN, a następnie skorzystać z tych informacji w celu rozwiązania problemów lub monitorowania.

Aby pobrać dzienniki urządzenia VPN

1. Na stronie **Łączność** kliknij ikonę koła zębatego obok urządzenia VPN.
2. Kliknij **Pobierz dziennik**.
3. [Opcjonalnie] Wybierz **Przechwytuj pakiety sieciowe** i skonfiguruj ustawienia. Aby uzyskać więcej informacji, zobacz "Przechwytywanie pakietów sieciowych" (s. 831).
4. Kliknij **Gotowe**.
5. Kiedy archiwum .zip będzie gotowe do pobrania, kliknij **Pobierz dziennik** i zapisz go lokalnie.

Pobieranie dzienników bramy VPN

Możesz pobrać i wyodrębnić archiwum zawierające dzienniki bramy VPN, a następnie skorzystać z tych informacji w celu rozwiązania problemów lub monitorowania.

Aby pobrać dzienniki bramy VPN

© Acronis International GmbH, 2003-2024

1. Na stronie **Łączność** kliknij ikonę koła zębatego obok bramy VPN.
2. Kliknij **Pobierz dziennik**.
3. [Opcjonalnie] Wybierz **Przechwytuj pakiety sieciowe**, a następnie skonfiguruj ustawienia. Aby uzyskać więcej informacji, zobacz "Przechwytywanie pakietów sieciowych" (s. 831).
4. Kliknij **Gotowe**.
5. Kiedy archiwum .zip będzie gotowe do pobrania, kliknij **Pobierz dziennik** i zapisz go lokalnie.

Przechwytywanie pakietów sieciowych

Z myślą o rozwiązywaniu problemów i analizowaniu komunikacji między lokalną lokalizacją produkcyjną a serwerem podstawowym lub serwerem odzyskiwania można wybrać opcję zbierania pakietów sieciowych na bramie VPN lub urządzeniu VPN.

Po zebraniu 32 000 pakietów sieciowych lub wyczerpaniu się limitu czasu przechwytywanie pakietów sieciowych zostanie zatrzymane, a wyniki zostaną zapisane w pliku .libpcap, który zostanie dodany do archiwum .zip dzienników.

Poniższa tabela zawiera dodatkowe informacje na temat ustawień funkcji **Przechwytuj pakiety sieciowe**, które można skonfigurować.

Ustawienie	Opis
Nazwa interfejsu sieciowego	Interfejs sieciowy, na którym mają być przechwytywane pakiety sieciowe. Jeśli pakiety sieciowe mają być przechwytywane na wszystkich interfejsach sieciowych, wybierz opcję **Dowolny**.
Limit czasu (w sekundach)	Limit czasu przechwytywania pakietów sieciowych. Wartość maksymalna to 1800.
Filtrowanie	Dodatkowy filtr do zastosowania do przechwytywanych pakietów sieciowych. Można wprowadzić ciąg obejmujący protokoły, porty i kierunki oraz ich kombinacje oddzielone spacją, takie jak: „and”, „or”, „not”, „ (”, „) ”, „src”, „dst”, „net”, „host”, „port”, „ip”, „tcp”, „udp”, „icmp”, „arp”, „esp”. Jeśli chcesz użyć nawiasu, dodaj przed nim i po nim spacje. Możesz też wprowadzić adresy IP i adresy sieciowe, na przykład: „icmp or arp” i „port 67 or 68”. Dodatkowe informacje na temat wartości, które można wprowadzić, można znaleźć w pomocy do narzędzia tpcdump w systemie Linux.

Rozwiązywanie problemów z konfiguracją IPsec VPN

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

© Acronis International GmbH, 2003-2024

Podczas konfigurowania połączenia IPsec VPN lub korzystania z niego mogą wystąpić pewne problemy.

Więcej informacji na temat napotkanych problemów można znaleźć w plikach dziennika IPsec, a w celu uzyskania możliwych rozwiązań niektórych często występujących problemów zapoznaj się z tematem „Rozwiązywanie napotkanych problemów z konfiguracją IPsec VPN”.

Rozwiązywanie napotkanych problemów z konfiguracją IPsec VPN

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W poniższej tabeli opisano najczęściej występujące problemy z konfiguracją IPsec VPN oraz wyjaśniono, jak je rozwiązać.

Problem	Możliwe rozwiązanie
Pojawił się następujący komunikat o błędzie: **Błąd negocjacji w fazie 1 IKE. Sprawdź ustawienia IPsec IKE w magazynie Cloud i lokalizacji lokalnej.**	Kliknij **Spróbuj ponownie** i sprawdź, czy pojawi się bardziej szczegółowy komunikat o błędzie. Bardziej szczegółowym komunikatem o błędzie może być na przykład komunikat o niezgodności algorytmów lub niepoprawnym kluczu PSK. **Uwaga** Ze względów bezpieczeństwa w przypadku łączności IPsec VPN występują następujące ograniczenia: • W dokumencie RFC8247 zaleca się wycofywanie protokołu IKEv1 i nie jest on obsługiwany ze względu na zagrożenia bezpieczeństwa. Obsługiwane są tylko połączenia przy użyciu protokołu IKEv2. • Następujące algorytmy szyfrowania nie są uznawane za bezpieczne i nie są obsługiwane: DES i 3DES. • Następujące algorytmy skrótów nie są uznawane za bezpieczne i nie są obsługiwane: SHA1 i MD5. • Liczba 2 z grupy Diffiego-Hellmana 2 nie jest uznawana za bezpieczną i nie jest obsługiwana.
Połączenie między moją lokalizacją lokalną a lokalizacją w chmurze stale ma status **Łączenie**.	Sprawdź, czy: • Port UDP 500 jest otwarty (jeśli korzystasz z zapory). • Jest łączność między lokalizacją lokalną a lokalizacją w chmurze.

© Acronis International GmbH, 2003-2024

Problem	Możliwe rozwiązanie
	• Adres IP lokalizacji lokalnej jest poprawny.
Połączenie między moją lokalizacją lokalną a lokalizacją w chmurze stale ma status **Oczekiwanie na połączenie**.	Status ten pojawia się, gdy opcja **Czynność podczas uruchamiania** w przypadku lokalizacji w chmurze ma ustawienie **Dodaj**, co oznacza, że lokalizacja w chmurze czeka, aż lokalizacja lokalna zainicjuje połączenie. Zainicjuj połączenie z lokalizacji lokalnej.
Połączenie między moją lokalizacją lokalną a lokalizacją w chmurze stale ma status **Oczekiwanie na ruch**.	Status ten pojawia się, gdy opcja **Czynność podczas uruchamiania** w przypadku lokalizacji w chmurze ma ustawienie **Przekieruj**. Jeśli oczekujesz na połączenie z lokalizacji lokalnej, zrób tak: • Z lokalizacji lokalnej spróbuj wysłać polecenie ping do maszyny wirtualnej w lokalizacji w chmurze. Jest to standardowe zachowanie niezbędne do ustanowienia tunelu w przypadku niektórych urządzeń, na przykład Cisco ASA. (Tryb przekierowania) • Zadbaj, aby lokalizacja lokalna utworzyła tunel, ustawiając jej **Czynność podczas uruchamiania** na **Rozpocznij**.
Połączenie między moją lokalizacją lokalną a lokalizacją w chmurze zostało nawiązane, ale co najmniej jedna z zasad sieciowych nie działa.	Ten problem może mieć jedną z następujących przyczyn: • Mapowanie sieci w lokalizacji IPsec w chmurze jest inne niż mapowanie sieci w lokalizacji lokalnej. Zadbaj, aby mapowania sieci i kolejność zasad sieciowych w lokalizacji lokalnej i lokalizacji w chmurze były dokładnie takie same. • Ten stan jest poprawny, gdy opcja **Czynność podczas uruchamiania** w przypadku lokalizacji lokalnej i/lub lokalizacji w chmurze ma ustawienie **Przekieruj** (na przykład na urządzeniach Cisco ASA), a w danej chwili nie ma ruchu. Spróbuj wysłać polecenie ping, aby sprawdzić, czy tunel został ustanowiony. Jeśli polecenie ping nie działa, sprawdź mapowanie sieci na lokalizacji lokalnej i lokalizacji w chmurze.
Chcę ponownie uruchomić wybrane	Aby ponownie uruchomić wybrane połączenie

© Acronis International GmbH, 2003-2024

Problem	Możliwe rozwiązanie
połączenie IPsec.	IPsec: 1. Na ekranie **Odzyskiwanie po awarii** > **Łączność** kliknij odpowiednie połączenie IPsec. 2. Kliknij **Wyłącz połączenie**. 3. Ponownie kliknij połączenie IPsec. 4. Kliknij **Włącz połączenie**.

Pobieranie plików dziennika IPsec VPN

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W plikach dziennika na serwerze VPN można znaleźć dodatkowe informacje na temat łączności IPsec. Pliki dziennika są skompresowane w archiwum .zip, które można pobrać i wyodrębnić.

Wymagania wstępne

Skonfigurowano łączność IPsec VPN multi-site.

Aby pobrać archiwum .zip z plikami dziennika

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij ikonę koła zębatego obok bramy VPN lokalizacji w chmurze.
3. Kliknij **Pobierz dziennik**.
4. Kliknij **Gotowe**.
5. Kiedy archiwum .zip będzie gotowe do pobrania, kliknij **Pobierz dziennik** i zapisz go lokalnie.

Pliki dziennika IPsec VPN multi-site

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Poniższa lista udostępnia opisy plików dzienników IPsec VPN zawartych w archiwum .zip oraz zawartych w nich informacji.

- `ip.txt` — ten plik zawiera dziennik konfiguracji kart sieciowych. Powinny być widoczne dwa adresy IP: publiczny adres IP i lokalny adres IP. Jeśli nie ma tych adresów IP w dzienniku, to znaczy, że wystąpił jakiś problem. Skontaktuj się z zespołem pomocy technicznej.

  Uwaga
  Maską publicznego adresu IP musi być 32.

- `swanctl-list-loaded-config.txt` — ten plik zawiera informacje o wszystkich lokalizacjach IPsec.

© Acronis International GmbH, 2003-2024

Jeśli w pliku nie ma lokalizacji, to konfiguracja IPsec nie została zastosowana. Spróbuj zaktualizować konfigurację i ją zapisać, lub skontaktuj się z zespołem pomocy technicznej.

- `swanctl-list-active-sas.txt` — ten plik zawiera połączenia i zasady ze statusem aktywności lub łączenia.

Konfigurowanie serwerów odzyskiwania

W tej sekcji omówiono pojęcia przełączania awaryjnego i powrotu po awarii, tworzenie serwera odzyskiwania oraz operacje odzyskiwania po awarii.

Tworzenie serwera odzyskiwania

Aby utworzyć serwer odzyskiwania, który będzie kopią obciążenia, możesz skorzystać z poniższej procedury. Możesz też obejrzeć instruktaż wideo, w którym pokazano cały ten proces.

Ważne
Podczas wykonywania przełączenia awaryjnego można wybrać tylko te punkty odzyskiwania, które zostały utworzone po utworzeniu serwera odzyskiwania.

Wymagania wstępne

- Do oryginalnego komputera, który chcesz chronić, musi być stosowany plan ochrony. W ramach planu w chmurze musi zostać utworzona kopia zapasowa całego komputera lub tylko dysków niezbędnych do uruchomienia komputera i udostępnienia potrzebnych usług.
- Trzeba ustawić typ łączności z lokalizacją w chmurze.

Aby stworzyć serwer odzyskiwania

1. Na karcie **Wszystkie urządzenia** wybierz komputer, który ma być chroniony.
2. Kliknij **Odzyskiwanie po awarii**, a następnie kliknij **Utwórz serwer odzyskiwania**.
3. Wybierz liczbę rdzeni wirtualnych i rozmiar pamięci RAM.

   Uwaga
   Podano liczbę punktów obliczeniowych wykorzystywanych w przypadku każdej opcji. Liczba punktów obliczeniowych odzwierciedla koszt działania serwera odzyskiwania przez godzinę. Aby uzyskać więcej informacji, zobacz "Punkty obliczeniowe" (s. 791).

4. Wskaż sieć w chmurze, do której ma zostać podłączony serwer.
5. Wybierz **DHCP**.

Opcja DHCP	Opis
Dostępne w lokalizacji w chmurze	Ustawienie domyślne. Adres IP serwera zostanie udostępniony przez automatycznie skonfigurowany serwer DHCP w chmurze.

© Acronis International GmbH, 2003-2024

Opcja DHCP	Opis
Niestandardowe	Adres IP serwera zostanie udostępniony przez Twój własny serwer DHCP w chmurze.

6. [Opcjonalnie] Podaj **adres MAC**.

   Adres MAC jest unikatowym identyfikatorem przypisanym do karty sieciowej serwera. W przypadku korzystania z niestandardowego serwera DHCP można go skonfigurować tak, aby zawsze przypisywał określone adresy IP do określonych adresów MAC. Dzięki temu serwer odzyskiwania zawsze otrzymuje ten sam adres IP. Można uruchamiać aplikacje, które mają licencje zarejestrowane na adres MAC.
7. Określ adres IP, który będzie znajdował się w sieci produkcyjnej serwera. Domyślnie używany jest adres IP pierwotnego komputera.

   Uwaga
   Jeśli korzystasz z serwera DHCP, dodaj ten adres IP do listy elementów wykluczonych serwera, aby uniknąć konfliktu adresów IP.

   W przypadku korzystania z niestandardowego serwera DHCP trzeba w polu **Adres IP w sieci produkcyjnej** podać ten sam adres, który został skonfigurowany na serwerze DHCP. W przeciwnym razie testowe przełączanie awaryjne nie będzie działać prawidłowo i nie będzie można się komunikować z serwerem przy użyciu publicznego adresu IP.
8. [Opcjonalnie] Zaznacz pole wyboru **Testowy adres IP**, a następnie wprowadź adres IP.

   Umożliwi to przetestowanie przełączania awaryjnego w odizolowanej sieci testowej i połączenie serwera odzyskiwania przy użyciu protokołu RDP lub SSH podczas testu przełączania awaryjnego. W trybie testowego przełączania awaryjnego brama VPN zastępuje testowy adres IP produkcyjnym adresem IP za pomocą protokołu NAT.

   Jeśli pole wyboru pozostanie niezaznaczone, dostęp do serwera będzie możliwy wyłącznie z poziomu konsoli.

   Uwaga
   Jeśli korzystasz z serwera DHCP, dodaj ten adres IP do listy elementów wykluczonych serwera, aby uniknąć konfliktu adresów IP.

   Możesz wybrać jeden z sugerowanych adresów IP lub wprowadzić inny.
9. [Opcjonalnie] Zaznacz pole wyboru **Dostęp do Internetu**.

   Opcja ta pozwala serwerowi odzyskiwania na dostęp do Internetu podczas prawdziwego lub testowego przełączania awaryjnego. Domyślnie port TCP 25 jest otwarty dla połączeń wychodzących do publicznych adresów IP.
10. [Opcjonalnie] Ustaw **Próg RPO**.

    Próg RPO określa maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania nadającym się do wykorzystania do przełączania awaryjnego a czasem bieżącym. Można ustawić wartość z przedziałów: 15– 60 minut, 1–24 godz., 1–14 dni.

© Acronis International GmbH, 2003-2024

11. [Opcjonalnie] Zaznacz pole wyboru **Użyj publicznego adresu IP**.
    Publiczny adres IP serwera czyni go dostępnym w Internecie podczas prawdziwego lub testowego przełączania awaryjnego. Jeśli pole wyboru pozostanie niezaznaczone, serwer będzie dostępny wyłącznie w Twojej sieci produkcyjnej.
    Opcja **Użyj publicznego adresu IP** wymaga włączenia opcji **Dostęp do Internetu**.
    Publiczny adres IP zostanie wyświetlony po zakończeniu konfiguracji. Domyślnie port TCP 443 jest otwarty dla połączeń przychodzących do publicznych adresów IP.

    Uwaga
    Jeśli wyczyścisz pole wyboru **Użyj publicznego adresu IP** lub usuniesz serwer odzyskiwania, jego publiczny adres IP nie zostanie zastrzeżony.

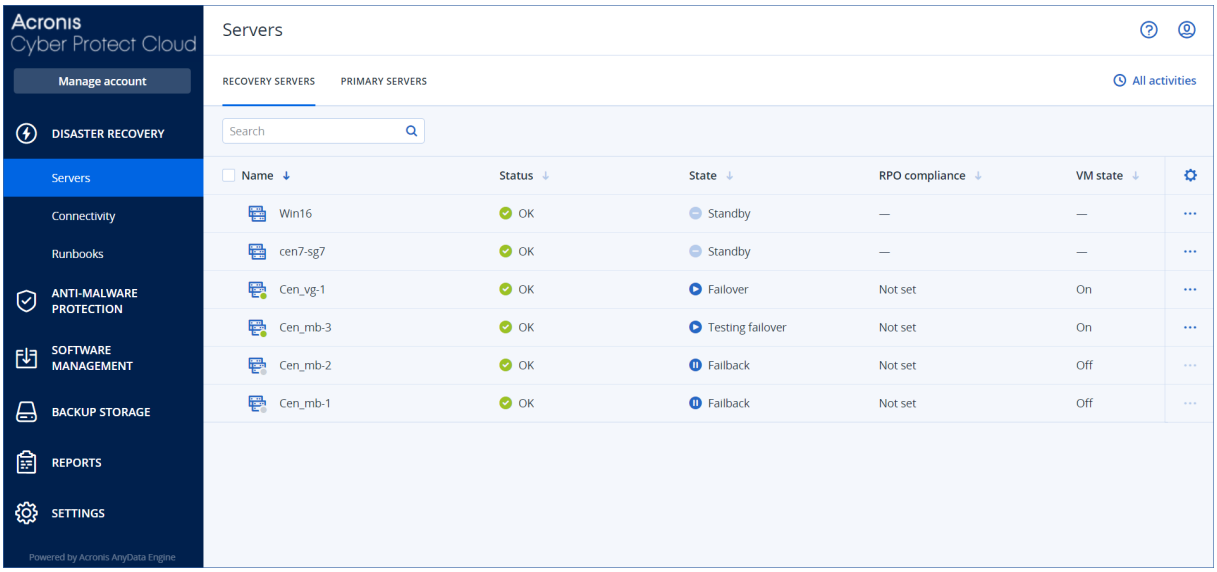
12. [Opcjonalnie] [Jeśli kopie zapasowe wybranego komputera są szyfrowane za pomocą szyfrowania jako właściwości komputera], określ hasło, które zostanie automatycznie użyte podczas tworzenia maszyny wirtualnej na potrzeby serwera odzyskiwania z zaszyfrowanej kopii zapasowej.
    a. Kliknij **Określ**, a następnie wprowadź hasło do zaszyfrowanej kopii zapasowej i zdefiniuj nazwę poświadczeń.
       Domyślnie na liście będzie wyświetlana najnowsza kopia zapasowa.
    b. [Opcjonalnie] Aby wyświetlić wszystkie kopie zapasowe, zaznacz **Pokaż wszystkie kopie zapasowe**.
    c. Kliknij **Gotowe**.

    Uwaga
    Wprawdzie określone hasło będzie przechowywane w bezpiecznym magazynie poświadczeń, jednak zapisywanie haseł może być sprzeczne z wymogami dotyczącymi zachowania zgodności z przepisami.

13. [Opcjonalnie] Zmień nazwę serwera odzyskiwania.
14. [Opcjonalnie] Wpisz opis serwera odzyskiwania.
15. [Opcjonalnie] Kliknij kartę **Reguły zapory chmury**, aby edytować domyślne reguły zapory. Aby uzyskać więcej informacji, zobacz "Ustawianie reguł zapory dla serwerów chmurowych" (s. 864).
16. Kliknij **Utwórz**.

Serwer odzyskiwania pojawi się na karcie **Odzyskiwanie po awarii** > **Serwery** > **Serwery odzyskiwania** konsoli Cyber Protect. Aby wyświetlić jego ustawienia, możesz zaznaczyć oryginalny komputer i kliknąć **Odzyskiwanie po awarii**.

© Acronis International GmbH, 2003-2024



Przebieg przełączania awaryjnego

Produkcyjne przełączanie awaryjne

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Gdy zostanie utworzony serwer odzyskiwania, działa on w **stanie gotowości**. Odpowiadająca mu maszyna wirtualna nie istnieje, dopóki nie zostanie rozpoczęte przełączanie awaryjne. Przed uruchomieniem przełączania awaryjnego trzeba utworzyć co najmniej jedną kopię zapasową obrazu dysku (z woluminem startowym) pierwotnego komputera.

Po rozpoczęciu przełączania awaryjnego wybierz punkt odzyskiwania (kopię zapasową) pierwotnego komputera, na podstawie którego zostanie utworzona maszyna wirtualna o uprzednio zdefiniowanych parametrach. W operacji przełączania awaryjnego używana jest funkcja „Uruchamianie maszyny wirtualnej z kopii zapasowej". Serwer odzyskiwania wchodzi w stan przejściowy **Finalizacja**. Proces ten polega na przeniesieniu dysków wirtualnych serwera z magazynu kopii zapasowych (pamięci „cold storage") do magazynu odzyskiwania po awarii (pamięci „hot storage").

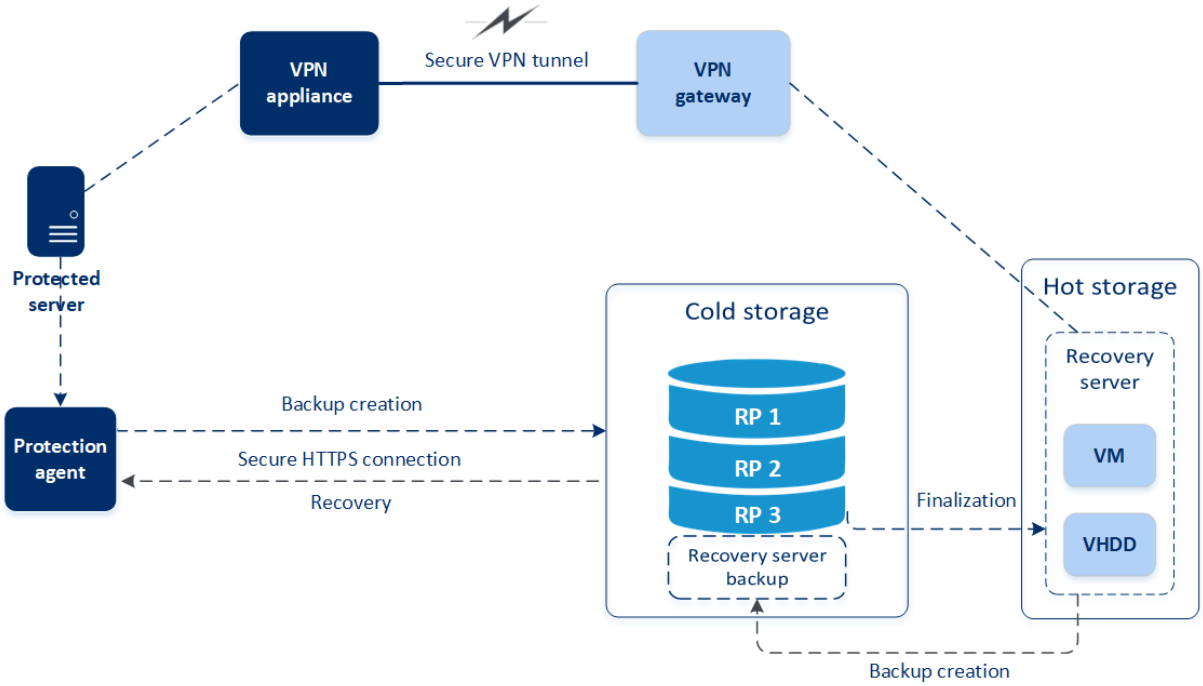
Uwaga
W trakcie procesu **Finalizacja** serwer jest dostępny i może wykonywać operacje, ale jego wydajność jest niższa niż zwykle. Możesz otworzyć konsolę serwera, klikając łącze **Konsola jest gotowa**. Łącze to jest dostępne w kolumnie **Stan maszyny wirtualnej** na ekranie **Odzyskiwanie po awarii** > **Serwery**, a także w widoku **Szczegóły** serwera.

Gdy **Finalizacja** zostanie ukończona, wydajność serwera osiąga normalną wartość. Stan serwera zmienia się na **Przełączanie awaryjne**. Obciążenie zostaje przełączone z oryginalnego komputera na serwer odzyskiwania w chmurze.

© Acronis International GmbH, 2003-2024

Jeśli na serwerze odzyskiwania znajduje się agent ochrony, usługa tego agenta jest zatrzymywana, aby zapobiec zakłóceniom (takim jak rozpoczęcie tworzenia kopii zapasowej lub zgłoszenie nieaktualnych statusów do komponentu kopii zapasowych).

Na poniższym diagramie przedstawiono zarówno proces przełączania awaryjnego, jak i proces powrotu po awarii.



Testuj przełączenie awaryjne

Podczas **testowego przełączania awaryjnego** maszyna wirtualna nie jest finalizowana. Oznacza to, że agent odczytuje zawartość dysków wirtualnych bezpośrednio z kopii zapasowej, tj. losowo uzyskuje dostęp do różnych części kopii zapasowej, i jego wydajność może być niższa od normalnej. Dodatkowe informacje na temat testowego przełączania awaryjnego można znaleźć w sekcji "Wykonywanie testowego przełączenia awaryjnego" (s. 839).

Automatyczne testowe przełączanie awaryjne

Skonfigurowane automatyczne testowe przełączanie awaryjne jest wykonywane raz w miesiącu bez jakichkolwiek ręcznych interakcji. Dodatkowe informacje można znaleźć w sekcjach "Automatyczne testowe przełączanie awaryjne" (s. 842) i "Konfigurowanie automatycznego testowego przełączania awaryjnego" (s. 843).

Wykonywanie testowego przełączenia awaryjnego

Wykonanie testu przełączania awaryjnego polega na uruchomieniu serwera odzyskiwania w testowej sieci VLAN odizolowanej od sieci produkcyjnej. Można przetestować kilka serwerów odzyskiwania jednocześnie i sprawdzić interakcje między nimi. W obrębie sieci testowej serwery

© Acronis International GmbH, 2003-2024

komunikują się za pomocą swoich produkcyjnych adresów IP, jednak nie mogą nawiązywać połączeń TCP ani UDP z obciążeniami w sieci lokalnej.

Podczas testowego przełączania awaryjnego maszyna wirtualna (serwer odzyskiwania) nie jest finalizowana. Agent odczytuje zawartość dysków wirtualnych bezpośrednio z kopii zapasowej i losowo uzyskuje dostęp do różnych części kopii zapasowej. Może to spowodować, że wydajność serwera odzyskiwania w stanie testowego przełączania awaryjnego będzie niższa od normalnej.

Wykonanie testu przełączania awaryjnego jest wprawdzie opcjonalne, jednak warto robić go regularnie — tak często, jak się da, biorąc pod uwagę koszty i względy bezpieczeństwa. Dobrą praktyką jest utworzenie runbooka, czyli zestawu instrukcji opisujących sposób uruchamiania środowiska produkcyjnego w chmurze.

Ważne
Trzeba zawczasu utworzyć serwer odzyskiwania, aby chronić swoje urządzenia przed awarią.

Przełączenie awaryjne można wykonać tylko z tych punktów odzyskiwania, które zostały utworzone po utworzeniu serwera odzyskiwania danego urządzenia.

Przed przełączeniem awaryjnym na serwer odzyskiwania musi zostać utworzony co najmniej jeden punkt odzyskiwania. Obsługiwanych jest maksymalnie 100 punktów odzyskiwania.

Aby wykonać testowe przełączenie awaryjne

1. Wybierz pierwotną maszynę lub serwer odzyskiwania, który chcesz przetestować.
2. Kliknij **Odzyskiwanie po awarii**.
   Zostanie wyświetlony opis serwera odzyskiwania.
3. Kliknij **Przełączanie awaryjne**.
4. Wybierz typ przełączania awaryjnego **Testuj przełączenie awaryjne**.
5. Wybierz punkt odzyskiwania (kopię zapasową), a następnie kliknij **Rozpocznij**.
6. Jeśli wybrana kopia zapasowa jest zaszyfrowana za pomocą szyfrowania jako właściwość komputera:
   a. Wprowadź hasło szyfrowania zestawu kopii zapasowych.

      Uwaga
      Hasło zostanie zapisane tylko tymczasowo i będzie używane tylko w ramach bieżącej operacji testowego przełączania awaryjnego. Jeśli testowe przełączanie awaryjne zostanie zatrzymane lub gdy się zakończy, hasło zostanie automatycznie usunięte z magazynu poświadczeń.

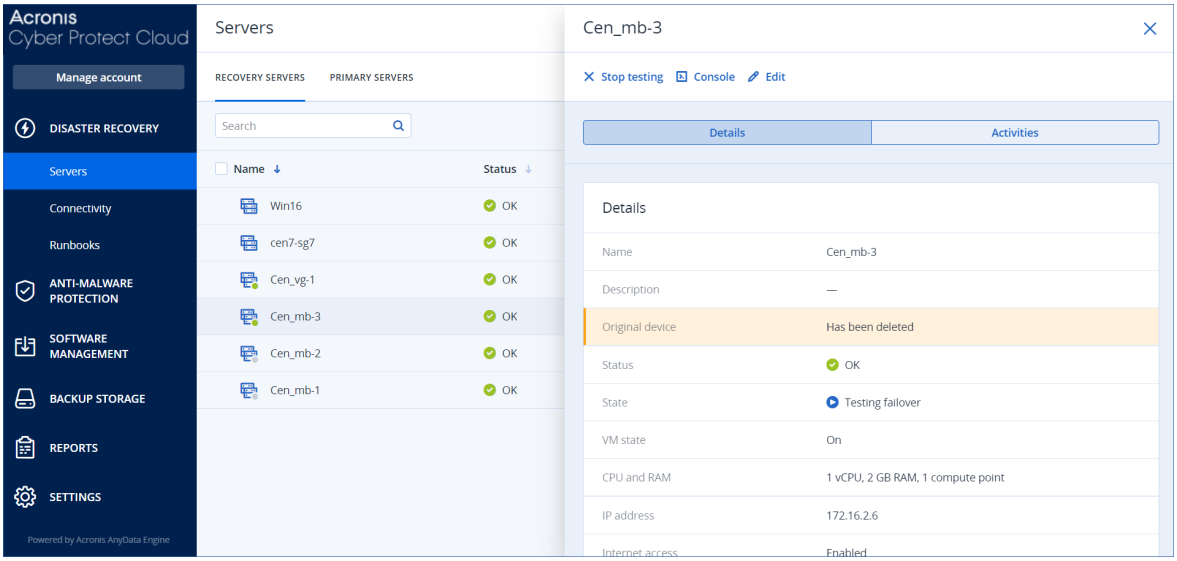
   b. [Opcjonalnie] Aby zapisać hasło do zestawu kopii zapasowych i użyć go w kolejnych operacjach przełączania awaryjnego, zaznacz pole wyboru **Zachowaj hasło w bezpiecznym magazynie poświadczeń**, a następnie w polu **Nazwa poświadczenia** wpisz nazwę tego poświadczenia.

© Acronis International GmbH, 2003-2024

Ważne
Hasło zostanie zapisane w bezpiecznym magazynie poświadczeń i będzie stosowane automatycznie w późniejszych operacjach przełączania awaryjnego. Zapisywanie haseł jednak może być sprzeczne z wymogami dotyczącymi zachowania zgodności z przepisami.

c. Kliknij **Gotowe**.

Po uruchomieniu serwera odzyskiwania jego stan zmieni się na **Testowanie przełączania awaryjnego**.



7. Wykonaj dowolne z następujących czynności, aby przetestować serwer odzyskiwania:
   - W sekcji **Odzyskiwanie po awarii** > **Serwery** wybierz serwer odzyskiwania, a następnie kliknij **Konsola**.
   - Nawiąż połączenie z serwerem odzyskiwania za pomocą protokołu RDP lub SSH oraz testowego adresu IP podanego podczas tworzenia tego serwera. Sprawdź połączenie zarówno wewnątrz sieci produkcyjnej, jak i poza nią (zgodnie z opisem podanym w sekcji „Połączenie point-to-site”).
   - Uruchom skrypt na serwerze odzyskiwania.

     Skrypt może sprawdzić ekran logowania, stan uruchomienia aplikacji, połączenie z Internetem oraz możliwość nawiązania połączenia z serwerem odzyskiwania przez pozostałe komputery.
   - Jeśli serwer odzyskiwania ma dostęp do Internetu i publiczny adres IP, można skorzystać z programu TeamViewer.
8. Po ukończeniu testu kliknij **Zatrzymaj testowanie**.

   Serwer odzyskiwania zostanie zatrzymany. Zmiany wprowadzone na serwerze odzyskiwania podczas testu przełączania awaryjnego nie są zapisywane.

© Acronis International GmbH, 2003-2024

Uwaga
Czynności **Uruchom serwer** i **Zatrzymaj serwer** nie mają zastosowania w przypadku operacji przełączania awaryjnego — dotyczy to zarówno runbooków, jak i ręcznego uruchomienia testowego przełączania awaryjnego. Próba wykonania takiej czynności zakończy się niepowodzeniem z następującym komunikatem o błędzie:
Niepowodzenie: Czynność nie ma zastosowania w bieżącym stanie serwera.

Automatyczne testowe przełączanie awaryjne

W przypadku korzystania z funkcji automatycznego testowego przełączania awaryjnego serwer odzyskiwania jest automatycznie testowany raz w miesiącu bez jakichkolwiek ręcznych interakcji.

Proces automatycznego testowego przełączania awaryjnego obejmuje następujące etapy:

1. utworzenie maszyny wirtualnej z ostatniego punktu odzyskiwania
2. wykonanie zrzutu ekranu maszyny wirtualnej
3. przeanalizowanie, czy system operacyjny maszyny wirtualnej pomyślnie się uruchamia
4. wysłanie powiadomienia o statusie testowego przełączania awaryjnego

Uwaga
Podczas automatycznego testowego przełączania awaryjnego wykorzystywane są punkty obliczeniowe.

Automatyczne testowe przełączanie awaryjne można skonfigurować w ustawieniach serwera odzyskiwania. Aby uzyskać więcej informacji, zobacz "Konfigurowanie automatycznego testowego przełączania awaryjnego" (s. 843).

Należy pamiętać, że w bardzo rzadkich przypadkach automatyczne testowe przełączanie awaryjne może zostać pominięte i nie zostać wykonane w zaplanowanym czasie. Może się tak zdarzyć, ponieważ przełączanie awaryjne w środowisku produkcyjnym ma wyższy priorytet niż automatyczne testowe przełączanie awaryjne, więc zasoby sprzętowe (procesor i pamięć RAM) alokowane na potrzeby automatycznego testowego przełączania awaryjnego mogą zostać tymczasowo ograniczone, aby wykonywane równolegle przełączanie awaryjne w środowisku produkcyjnym miało do dyspozycji wystarczające zasoby.

Jeśli automatyczne testowe przełączanie awaryjne zostanie z jakiegoś powodu pominięte, zostanie zgłoszony alert.

Uwaga
Automatyczne testowe przełączanie awaryjne się nie powiedzie, jeśli kopie zapasowe oryginalnego komputera są zaszyfrowane za pomocą szyfrowania jako właściwości komputera, a hasło szyfrowania nie zostało określone podczas tworzenia serwera odzyskiwania. Aby uzyskać więcej informacji na temat określania hasła szyfrowania, zobacz "Tworzenie serwera odzyskiwania" (s. 835).

© Acronis International GmbH, 2003-2024

Konfigurowanie automatycznego testowego przełączania awaryjnego

Dzięki skonfigurowaniu automatycznego testowego przełączania awaryjnego można co miesiąc testować serwer odzyskiwania bez ręcznego wykonywania jakichkolwiek czynności.

Aby skonfigurować automatyczne testowe przełączanie awaryjne

1. W konsoli przejdź do sekcji **Odzyskiwanie po awarii** > **Serwery** > **Serwery odzyskiwania** i zaznacz serwer odzyskiwania.
2. Kliknij **Edytuj**.
3. W sekcji **Automatyczne testowe przełączanie awaryjne** w polu **Harmonogram** wybierz **Co miesiąc**.
4. [Opcjonalnie] W polu **Limit czasu zrzutu ekranu** zmień wartość domyślną maksymalnego przedziału czasu (w minutach), w którym system będzie próbował wykonać automatyczne testowe przełączenie awaryjne.
5. [Opcjonalnie] Jeśli chcesz zapisać wartość pola **Limit czasu zrzutu ekranu** jako domyślną, tak aby była automatycznie stosowana, gdy aktywujesz automatyczne testowe przełączanie awaryjne dla innych serwerów odzyskiwania, wybierz **Ustaw jako domyślny limit czasu**.
6. Kliknij **Zapisz**.

Wyświetlanie statusu automatycznego testowego przełączania awaryjnego

Możesz wyświetlić szczegóły zakończonego automatycznego testowego przełączania awaryjnego, takie jak status, godzina rozpoczęcia, godzina zakończenia, czas trwania oraz zrzut ekranu maszyny wirtualnej.

Aby wyświetlić status automatycznego testowego przełączania awaryjnego serwera odzyskiwania

1. W konsoli przejdź do sekcji **Odzyskiwanie po awarii** > **Serwery** > **Serwery odzyskiwania** i zaznacz serwer odzyskiwania.
2. W sekcji **Automatyczne testowe przełączanie awaryjne** sprawdź szczegóły ostatniego automatycznego testowego przełączania awaryjnego.
3. [Opcjonalnie] Kliknij **Pokaż zrzut ekranu**, aby wyświetlić zrzut ekranu maszyny wirtualnej.

Wyłączanie automatycznego testowego przełączania awaryjnego

Automatyczne testowe przełączanie awaryjne można wyłączyć, aby oszczędzać zasoby lub jeśli automatyczne testowe przełączanie awaryjne nie musi zostać wykonane w przypadku określonego serwera odzyskiwania.

Aby wyłączyć automatyczne testowe przełączanie awaryjne

1. W konsoli przejdź do sekcji **Odzyskiwanie po awarii** > **Serwery** > **Serwery odzyskiwania** i zaznacz serwer odzyskiwania.
2. Kliknij **Edytuj**.

© Acronis International GmbH, 2003-2024

3. W sekcji **Automatyczne testowe przełączanie awaryjne** w polu **Harmonogram** wybierz **Nigdy**.
4. Kliknij **Zapisz**.

Wykonywanie przełączenia awaryjnego

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Przełączenie awaryjne to proces przenoszenia obciążenia z Twojej lokalizacji do chmury oraz stan obecności tego obciążenia w chmurze.

Po rozpoczęciu procesu przełączania awaryjnego serwer odzyskiwania jest uruchamiany w sieci produkcyjnej. Aby uniknąć zakłóceń i niepożądanych problemów, upewnij się, że pierwotne obciążenie nie jest w trybie online i nie ma do niego dostępu przez połączenie VPN.

Aby zapobiec zakłóceniom kopii zapasowych w tym samym archiwum w chmurze, należy ręcznie odwołać plan ochrony z obciążenia będącego aktualnie w stanie **Przełączanie awaryjne**. Dodatkowe informacje na temat odwoływania planów można znaleźć w sekcji Odwoływanie planu ochrony.

Ważne
Trzeba zawczasu utworzyć serwer odzyskiwania, aby chronić swoje urządzenia przed awarią.

Przełączenie awaryjne można wykonać tylko z tych punktów odzyskiwania, które zostały utworzone po utworzeniu serwera odzyskiwania danego urządzenia.

Przed przełączeniem awaryjnym na serwer odzyskiwania musi zostać utworzony co najmniej jeden punkt odzyskiwania. Obsługiwanych jest maksymalnie 100 punktów odzyskiwania.

Możesz postąpić zgodnie z poniższymi instrukcjami lub obejrzeć instruktaż wideo.

Aby wykonać przełączenie awaryjne

1. Upewnij się, że pierwotna maszyna nie jest dostępna w sieci.
2. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Serwery** > **Serwery odzyskiwania** i zaznacz serwer odzyskiwania.
3. Kliknij **Przełączanie awaryjne**.
4. Wybierz typ przełączania awaryjnego **Produkcyjne przełączanie awaryjne**.
5. Wybierz punkt odzyskiwania (kopię zapasową), a następnie kliknij **Rozpocznij**.
6. [Jeśli wybrana kopia zapasowa jest zaszyfrowana za pomocą szyfrowania jako właściwość komputera]

© Acronis International GmbH, 2003-2024

a. Wprowadź hasło szyfrowania zestawu kopii zapasowych.

Uwaga
Hasło zostanie zapisane tylko tymczasowo i będzie używane tylko w ramach bieżącej operacji przełączania awaryjnego. Po zakończeniu operacji przełączania awaryjnego i powrocie serwera do stanu **Stan gotowości** hasło zostanie automatycznie usunięte z magazynu poświadczeń.

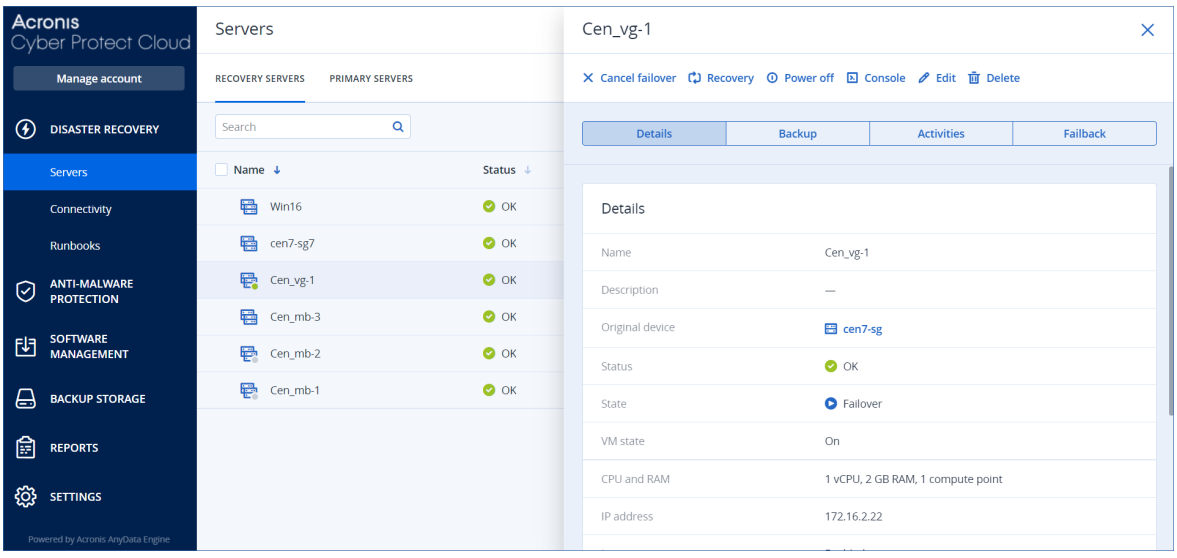
b. [Opcjonalnie] Aby zapisać hasło do zestawu kopii zapasowych i użyć go w kolejnych operacjach przełączania awaryjnego, zaznacz pole wyboru **Zachowaj hasło w bezpiecznym magazynie poświadczeń**, a następnie w polu **Nazwa poświadczenia** wpisz nazwę tego poświadczenia.

Ważne
Hasło zostanie zapisane w bezpiecznym magazynie poświadczeń i będzie stosowane automatycznie w późniejszych operacjach przełączania awaryjnego. Zapisywanie haseł jednak może być sprzeczne z wymogami dotyczącymi zachowania zgodności z przepisami.

c. Kliknij **Gotowe**.

Po uruchomieniu serwera odzyskiwania jego stan zmienia się na **Finalizacja**, a po pewnym czasie na **Przełączanie awaryjne.**

Ważne
Nie wolno zapominać, że serwer jest dostępny zarówno w stanie **Finalizacja**, jak i w stanie **Przełączanie awaryjne**. W stanie **Finalizacja** można uzyskać dostęp do konsoli serwera przez kliknięcie łącza **Konsola jest gotowa**. Łącze to jest dostępne w kolumnie **Stan maszyny wirtualnej** na ekranie **Odzyskiwanie po awarii** > **Serwery**, a także w widoku **Szczegóły** serwera. Szczegółowe informacje można znaleźć w sekcji "Przebieg przełączania awaryjnego" (s. 838).



© Acronis International GmbH, 2003-2024

7. Upewnij się, że serwer odzyskiwania został uruchomiony, sprawdzając jego konsolę. Kliknij **Odzyskiwanie po awarii** > **Serwery**, wybierz serwer odzyskiwania, a następnie kliknij **Konsola**.
8. Upewnij się, że do serwera odzyskiwania można uzyskać dostęp za pomocą produkcyjnego adresu IP podanego podczas tworzenia tego serwera.

Po sfinalizowaniu serwera odzyskiwania automatycznie jest tworzony nowy plan ochrony i stosowany na tym serwerze. Ten plan ochrony jest tworzony na podstawie planu, za pomocą którego utworzono serwer odzyskiwania (z pewnymi ograniczeniami). W tym planie możesz zmienić tylko harmonogram oraz reguły przechowywania. Aby uzyskać więcej informacji, zobacz sekcję „Tworzenie kopii zapasowych serwerów chmurowych”.

Jeśli chcesz anulować przełączenie awaryjne, wybierz serwer odzyskiwania i kliknij **Anuluj przełączenie awaryjne**. Wszystkie zmiany wprowadzone od chwili przełączenia awaryjnego, z wyjątkiem kopii zapasowych serwera odzyskiwania, zostaną utracone. Serwer odzyskiwania wróci do stanu **gotowości**.

Jeśli chcesz wykonać powrót po awarii, wybierz serwer odzyskiwania i kliknij **Powrót po awarii**.

Jak wykonać przełączenie awaryjne serwerów korzystających z lokalnego serwera DNS

Jeśli używasz serwerów DNS w lokalizacji lokalnej do rozpoznawania nazw komputerów, to po przełączeniu awaryjnym na serwery odzyskiwania odpowiadające im komputery korzystające z serwerów DNS nie będą się komunikować, ponieważ w chmurze są używane inne serwery DNS. Domyślnie serwery DNS w lokalizacji chmurze są używane na potrzeby nowo utworzonych serwerów chmurowych. Jeśli trzeba zastosować niestandardowe ustawienia DNS, skontaktuj się z działem pomocy technicznej.

Jak wykonać przełączenie awaryjne serwera DHCP

Lokalna infrastruktura może obejmować serwer DHCP działający na komputerze z systemem Windows lub Linux. W przypadku przełączenia awaryjnego takiego hosta do lokalizacji w chmurze pojawia się problem zdublowania serwera DHCP, ponieważ brama VPN w chmurze pełni również funkcję serwera DHCP. Aby rozwiązać ten problem, wykonaj jedną z następujących czynności:

- Jeśli tylko host DHCP został przełączony awaryjnie do chmury, a pozostałe serwery lokalne nadal działają w lokalizacji lokalnej, zaloguj się na hoście DHCP w chmurze i wyłącz na nim serwer DHCP. W ten sposób zapobiegniesz konfliktom i tylko brama VPN będzie działać jako serwer DHCP.
- Jeśli serwery chmurowe mają już adresy IP z hosta DHCP, trzeba się zalogować na hoście DHCP w chmurze i wyłączyć na nim serwer DHCP. Trzeba też się zalogować na serwery chmurowe i odnowić dzierżawę DHCP, aby przypisać nowe adresy IP przydzielone z właściwego serwera DHCP (hostowanego na bramie VPN).

© Acronis International GmbH, 2003-2024

Uwaga
Instrukcje te nie mają zastosowania, jeśli serwer DHCP w chmurze jest skonfigurowany z użyciem opcji **Niestandardowy serwer DHCP**, a niektóre serwery odzyskiwania lub podstawowe dostają z niego swoje adresy IP.

Przebieg powrotu po awarii

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Powrót po awarii to proces przenoszenia obciążenia z chmury z powrotem na komputer fizyczny lub maszynę wirtualną w lokalizacji lokalnej. Można wykonać powrót po awarii na serwer odzyskiwania w stanie **Przełączanie awaryjne** i nadal korzystać z tego serwera w lokalizacji lokalnej.

Istnieje możliwość przeprowadzenia automatycznego przełączenia awaryjnego na docelowy komputer fizyczny w lokalizacji lokalnej. Podczas powrotu po awarii można przesłać dane kopii zapasowej do lokalizacji lokalnej, podczas gdy maszyna wirtualna w chmurze nadal działa. Technologia ta pozwala na uzyskanie bardzo krótkiego czasu przestoju, którego oszacowanie jest wyświetlane w konsoli Cyber Protect. Można je sprawdzić i uwzględnić w planach swoich działań, a także ostrzec klientów o zbliżającym się przestoju, jeśli jest taka potrzeba.

Procesy powrotu po awarii na docelowe maszyny wirtualne nieco się różnią od procesów powrotu po awarii na docelowe komputery fizyczne. Dodatkowe informacje na temat faz procesu powrotu po awarii można znaleźć w sekcjach "Powrót po awarii na docelową maszynę wirtualną" (s. 847) i "Powrót po awarii na docelowy komputer fizyczny" (s. 852).

W szczególnych przypadkach, gdy nie można zastosować procedury automatycznego powrotu po awarii, można wykonać tę operację ręcznie. Aby uzyskać więcej informacji, zobacz "Ręczny powrót po awarii" (s. 856).

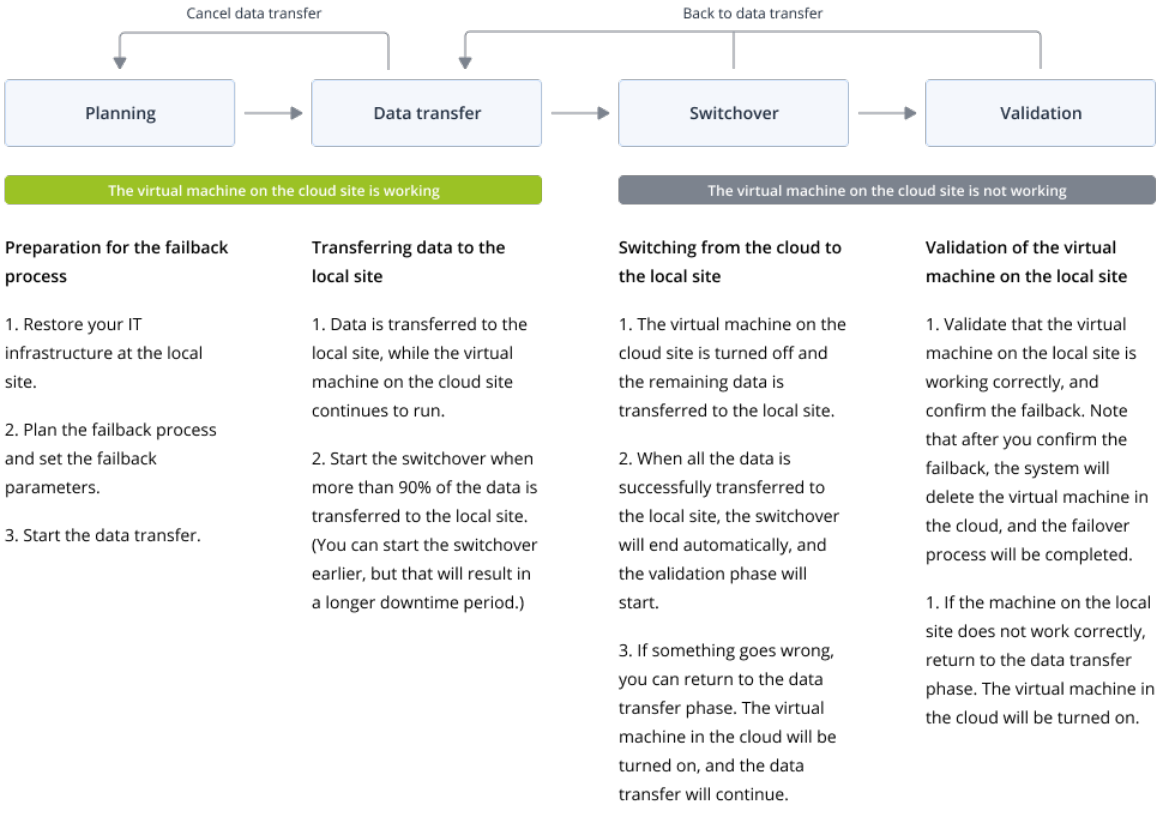
Uwaga
W przypadku wykonywania operacji przy użyciu runbooków jest obsługiwany tylko ręczny tryb powrotu po awarii. Oznacza to, że po rozpoczęciu powrotu po awarii przez wykonanie runbooka obejmującego krok **Powrót po awarii serwera** procedura będzie wymagała ręcznych interakcji: trzeba będzie ręcznie odzyskać komputer, a następnie potwierdzić lub anulować proces powrotu po awarii na karcie **Odzyskiwanie po awarii** > **Serwery**.

Powrót po awarii na docelową maszynę wirtualną

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Proces powrotu po awarii na docelową maszynę wirtualną obejmuje cztery fazy.

© Acronis International GmbH, 2003-2024



1. **Planowanie**. W tej fazie jest przywracana infrastruktura IT w lokalizacji lokalnej (taka jak hosty i konfiguracje sieci), są konfigurowane parametry powrotu po awarii i jest planowany czas rozpoczęcia przesyłania danych.

   Uwaga
   Aby zminimalizować czas trwania procesu powrotu po awarii, warto rozpocząć fazę przesyłania danych zaraz po skonfigurowaniu serwerów lokalnych i kontynuować konfigurowanie sieci oraz pozostałej infrastruktury lokalnej w trakcie fazy przesyłania danych.

2. **Przesyłanie danych**. W tej fazie dane są przesyłane z lokalizacji w chmurze do lokalizacji lokalnej, a maszyna wirtualna w chmurze nadal działa. W fazie przesyłania danych można w każdej chwili rozpocząć następną fazę, czyli przełączanie, ale warto wziąć pod uwagę następujące zależności:

   Im dłużej trwa faza przesyłania danych,

   - tym dłużej działa maszyna wirtualna w chmurze.
   - tym więcej danych zostanie przesłanych do lokalizacji lokalnej.
   - tym wyższe będą koszty (poświęcisz więcej punktów obliczeniowych).
   - tym krótszy będzie przestój w fazie przełączania.

   Jeśli chcesz maksymalnie skrócić czas przestoju, rozpocznij fazę przełączania, gdy do lokalizacji lokalnej zostanie przesłanych ponad 90% danych.

© Acronis International GmbH, 2003-2024

Jeśli możesz sobie pozwolić na dłuższy przestój, a nie chcesz wykorzystywać kolejnych punktów obliczeniowych na działanie maszyny wirtualnej w chmurze, możesz rozpocząć fazę przełączanie wcześniej.

Jeśli anulujesz proces powrotu po awarii w fazie przesyłania danych, to przesłane dane nie zostaną usunięte z lokalizacji lokalnej. Aby uniknąć ewentualnych problemów, ręcznie usuń przeniesione dane, zanim rozpoczniesz nowy proces powrotu po awarii. Kolejny proces przesyłania danych zacznie się od nowa.

3. **Przełączanie**. W tej fazie jest wyłączana maszyna wirtualna w chmurze, i pozostałe dane, w tym ostatni przyrost kopii zapasowej, są przesyłane do lokalizacji lokalnej. Jeśli na serwerze odzyskiwania nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, a to spowolni proces.

   Szacowany czas do zakończenia tej fazy (czas przestoju) można sprawdzić w konsoli Cyber Protect. Z chwilą przesłania wszystkich danych do lokalizacji lokalnej (nie wystąpi żadna utrata danych, a maszyna wirtualna w lokalizacji lokalnej będzie dokładną kopią maszyny wirtualnej z chmury) faza przełączania zostaje zakończona. Maszyna wirtualna w lokalnej lokalizacji będzie odzyskana i automatycznie się rozpocznie faza sprawdzania poprawności.
4. **Sprawdzenie poprawności**. W tej fazie maszyna wirtualna w lokalizacji lokalnej jest gotowa i zostaje automatycznie uruchomiona. Możesz sprawdzić, czy maszyna wirtualna działa poprawnie, a ponadto:
   - Jeśli wszystko działa zgodnie z oczekiwaniami, można potwierdzić wykonanie powrotu po awarii. Po potwierdzeniu wykonania powrotu po awarii zostaje usunięta maszyna wirtualna w chmurze, a serwer odzyskiwania wraca do stanu **Stan gotowości**. Na tym proces powrotu po awarii się kończy.
   - Jeśli coś będzie nie tak, można anulować przełączanie i wrócić do fazy przesyłania danych.

Wykonywanie powrotu po awarii na maszynę wirtualną

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Istnieje możliwość przeprowadzenia powrotu po awarii na docelową maszynę wirtualną w lokalizacji lokalnej.

Wymagania wstępne

- Agent, który zostanie użyty do wykonania powrotu po awarii, jest w trybie online i nie jest aktualnie używany do żadnej innej operacji powrotu po awarii.
- Masz stabilne połączenie z Internetem.
- Istnieje co najmniej jedna pełna kopia zapasowa maszyny wirtualnej w chmurze.

Aby wykonać powrót po awarii na maszynę wirtualną

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Serwery**.
2. Wybierz serwer odzyskiwania znajdujący się w stanie **przełączania awaryjnego**.
3. Kliknij kartę **Powrót po awarii**.
4. W sekcji **Parametry powrotu po awarii** wybierz opcję **Maszyna wirtualna** w polu **Miejsce docelowe** i skonfiguruj pozostałe parametry.

   Uwaga: domyślnie niektóre **Parametry powrotu po awarii** mają automatycznie ustawione proponowane wartości, ale można je zmienić.

   Poniższa tabela zawiera dodatkowe informacje na temat ustawień dostępnych w sekcji **Parametry powrotu po awarii**.

Parametr	Opis
Rozmiar kopii zapasowej	Ilość danych, które zostaną przesłane do lokalizacji lokalnej podczas procesu powrotu po awarii. Po rozpoczęciu procesu powrotu po awarii na docelową maszynę wirtualną wartość **Rozmiar kopii zapasowej** będzie się zwiększać w fazie przesyłania danych, ponieważ maszyna wirtualna w chmurze nadal będzie działać i generować nowe dane. Aby oszacować czas przestoju podczas procesu powrotu po awarii na docelową maszynę wirtualną, podziel 10% wartości **Rozmiar kopii zapasowej** (ponieważ zalecamy rozpoczęcie fazy przełączania po przesłaniu 90% danych do lokalizacji lokalnej) przez wartość szybkości połączenia z Internetem. **Uwaga** W przypadku jednoczesnego wykonywania kilku procesów powrotu po awarii wartość szybkości połączenia z Internetem będzie mniejsza.
Miejsce docelowe	Typ obciążenia w lokalizacji lokalnej, na które będzie odzyskiwany serwer chmurowy: **Maszyna wirtualna** lub **Komputer fizyczny**.
Lokalizacja komputera docelowego	Lokalizacja na potrzeby powrotu po awarii: host VMware ESXi lub Microsoft Hyper-V. Możesz wybrać dowolny z hostów, które mają agenta zarejestrowanego w usłudze Cyber Protection.
Agent	Agent, który będzie wykonywać operację powrotu po awarii. Wybranego agenta można używać w danym czasie w ramach tylko jednej operacji powrotu po awarii. Można wybrać agenta, który jest w trybie online i nie jest aktualnie używany na potrzeby innego procesu powrotu po awarii, jest w wersji obsługującej funkcję powrotu po awarii oraz ma prawa dostępu do kopii zapasowej. Uwaga: można zainstalować na hostach VMware ESXi kilka agentów i uruchomić osobny proces powrotu po awarii przy użyciu każdego z nich. W ten sposób można wykonywać kilka procesów powrotu po awarii naraz.

© Acronis International GmbH, 2003-2024

Parametr	Opis
Ustawienia komputera docelowego	Ustawienia maszyny wirtualnej: • **Procesory wirtualne**. Wybierz liczbę procesorów wirtualnych. • **Pamięć**. Wybierz wielkość pamięci maszyny wirtualnej. • **Jednostki**. Wybierz jednostki pamięci. • [Opcjonalnie] **Karty sieciowe**. Aby dodać kartę sieciową, kliknij **Dodaj** i w polu **Sieć** wybierz sieć. Po wprowadzeniu pożądanych zmian kliknij **Gotowe**.
Ścieżka	(W przypadku hostów Microsoft Hyper-V) Folder na hoście, na którym będzie rezydować maszyna. Upewnij się, że w pamięci hosta jest wystarczająco dużo wolnego miejsca na maszynę.
Magazyn danych	(W przypadku hostów VMware ESXi) Magazyn danych na hoście, na którym będzie rezydować maszyna. Upewnij się, że w pamięci hosta jest wystarczająco dużo wolnego miejsca na maszynę.
Tryb alokowania	Metoda alokacji dysku wirtualnego. W przypadku hostów Microsoft Hyper-V: • **Powiększający się dynamicznie** (wartość domyślna). • **Stały rozmiar**. W przypadku hostów Microsoft Hyper-V: • **Elastyczne** (wartość domyślna). • **Nieelastyczne**.
Nazwa komputera docelowego	Nazwa komputera docelowego. Domyślnie komputer docelowy ma taką samą nazwę jak serwer odzyskiwania. Nazwa komputera docelowego musi być unikatowa w ramach lokalizacji wybranej w polu **Lokalizacja komputera docelowego**.

5. Kliknij **Rozpocznij przesyłanie danych**, a następnie w oknie potwierdzenia kliknij **Rozpocznij**.

Uwaga
Jeżeli w chmurze nie ma kopii zapasowej maszyny wirtualnej, system automatycznie wykona kopię zapasową przed fazą przesyłania danych.

Rozpocznie się faza **Przesyłanie danych**. W konsoli będą wyświetlane następujące informacje:

Pole	Opis
Postęp	Ten parametr odzwierciedla ilość danych już przesłanych do lokalizacji lokalnej oraz całkowitą ilość danych do przesłania. Całkowita ilość danych obejmuje dane z ostatniej kopii zapasowej sprzed rozpoczęcia fazy przesyłania danych oraz kopie zapasowe nowo

© Acronis International GmbH, 2003-2024

Pole	Opis
	wygenerowanych danych (przyrosty kopii zapasowych), ponieważ maszyna wirtualna nadal działa podczas fazy przesyłania danych. Dlatego obie wartości parametru **Postęp** rosną w miarę upływu czasu.
Oszacowanie przestoju	Ten parametr wskazuje, jak długo maszyna wirtualna w chmurze będzie niedostępna w przypadku rozpoczęcia fazy przełączania w danej chwili. Wartość ta jest obliczana na podstawie wartości parametru **Postęp** i maleje w miarę upływu czasu.

6. Kliknij **Przełączanie**, a następnie w oknie potwierdzenia ponownie kliknij **Przełączanie**.
   Rozpocznie się faza przełączania. W konsoli będą wyświetlane następujące informacje:

Pole	Opis
Postęp	Ten parametr ilustruje postęp przywracania maszyny w lokalizacji lokalnej.
Szacowany czas do końca	Ten parametr ilustruje przybliżony czas zakończenia fazy przełączania, kiedy to będzie można włączyć komputer w lokalizacji lokalnej.

Uwaga
Jeśli do maszyny wirtualnej w chmurze nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, co spowoduje dłuższy przestój.

7. Po zakończeniu fazy **Przełączanie** i automatycznym uruchomieniu maszyny wirtualnej w lokalizacji lokalnej sprawdź, czy działa ona zgodnie z oczekiwaniami.
8. Kliknij **Potwierdź powrót po awarii**, a następnie w oknie potwierdzenia kliknij **Potwierdź**, aby sfinalizować proces.
   Maszyna wirtualna w chmurze zostaje usunięta, a serwer odzyskiwania wraca do stanu **Stan gotowości**.

Uwaga
Zastosowanie planu ochrony na odzyskiwanym serwerze nie jest częścią procesu powrotu po awarii. Po zakończeniu procesu powrotu po awarii zastosuj plan ochrony na odzyskanym serwerze, aby wznowić jego ochronę. Możesz wykorzystać ten sam plan ochrony, który został zastosowany na pierwotnym serwerze, lub nowy plan ochrony z włączonym modułem **Odzyskiwanie po awarii**.

Powrót po awarii na docelowy komputer fizyczny

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

© Acronis International GmbH, 2003-2024

Proces automatycznego powrotu po awarii na docelowy komputer fizyczny obejmuje następujące fazy:

1. **Planowanie**. W tej fazie jest przywracana infrastruktura IT w lokalizacji lokalnej (taka jak hosty i konfiguracje sieci), są konfigurowane parametry powrotu po awarii i jest planowany czas rozpoczęcia przesyłania danych.
2. **Przesyłanie danych**. W tej fazie dane są przesyłane z lokalizacji w chmurze do lokalizacji lokalnej, a maszyna wirtualna w chmurze nadal działa. W fazie przesyłania danych można w każdej chwili rozpocząć następną fazę, czyli przełączanie, ale warto wziąć pod uwagę następujące zależności:

   Im dłużej trwa faza przesyłania danych,
   - tym dłużej działa maszyna wirtualna w chmurze.
   - tym więcej danych zostanie przesłanych do lokalizacji lokalnej.
   - tym wyższe będą koszty (poświęcisz więcej punktów obliczeniowych).
   - tym krótszy będzie przestój w fazie przełączania.

   Jeśli chcesz maksymalnie skrócić czas przestoju, rozpocznij fazę przełączania, gdy do lokalizacji lokalnej zostanie przesłanych ponad 90% danych.

   Jeśli możesz sobie pozwolić na dłuższy przestój, a nie chcesz wykorzystywać kolejnych punktów obliczeniowych na działanie maszyny wirtualnej w chmurze, możesz rozpocząć fazę przełączanie wcześniej.

   Uwaga
   Proces przesyłania danych wykorzystuje technologię flashback. Technologia ta obsługuje porównanie danych dostępnych na komputerze docelowym z danymi na maszynie wirtualnej w chmurze. Jeśli część tych danych jest już dostępna na komputerze docelowym, nie zostaną one przesłane ponownie. Technologia ta przyspiesza realizację fazy Przesyłanie danych.
   Dlatego zalecamy przywrócenie serwera na pierwotną maszynę w lokalizacji lokalnej.

3. **Przełączanie**. W tej fazie jest wyłączana maszyna wirtualna w chmurze, i pozostałe dane, w tym ostatni przyrost kopii zapasowej, są przesyłane do lokalizacji lokalnej. Jeśli na serwerze odzyskiwania nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, a to spowolni proces.
4. **Sprawdzanie poprawności**. Podczas tej fazy komputer fizyczny w lokalizacji lokalnej jest gotowy i można go uruchomić ponownie przy użyciu nośnika startowego opartego na systemie Linux. Można sprawdzić, czy maszyna wirtualna działa poprawnie, oraz:
   - Jeśli wszystko działa zgodnie z oczekiwaniami, można potwierdzić wykonanie powrotu po awarii. Po potwierdzeniu wykonania powrotu po awarii zostaje usunięta maszyna wirtualna w chmurze, a serwer odzyskiwania wraca do stanu **Stan gotowości**. Na tym proces powrotu po awarii się kończy.
   - Jeśli coś będzie nie tak, można anulować przełączanie awaryjne i wrócić do fazy planowania.

© Acronis International GmbH, 2003-2024

Uwaga

Po ponownym uruchomieniu nośnika startowego nie będzie można go ponownie użyć. Jeśli w fazie sprawdzania poprawności zostanie wykryty jakiś błąd, trzeba będzie zarejestrować nowy nośnik startowy i ponownie rozpocząć proces powrotu po awarii.

Ponieważ jednak będzie używana technologia flashback, dane, które już się znajdują w lokalizacji lokalnej, nie będą ponownie przesyłane, a proces powrotu po awarii będzie znacznie szybszy.

Wykonywanie powrotu po awarii na komputer fizyczny

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Istnieje możliwość automatycznego przeprowadzenia powrotu po awarii na docelowy komputer fizyczny w lokalizacji lokalnej.

Uwaga

Proces przesyłania danych wykorzystuje technologię flashback. Technologia ta obsługuje porównanie danych dostępnych na komputerze docelowym z danymi na maszynie wirtualnej w chmurze. Jeśli część tych danych jest już dostępna na komputerze docelowym, nie zostaną one przesłane ponownie. Technologia ta przyspiesza realizację fazy Przesyłanie danych.

Dlatego zalecamy przywrócenie serwera na pierwotną maszynę w lokalizacji lokalnej.

Wymagania wstępne

- Agent, który zostanie użyty do wykonania powrotu po awarii, jest w trybie online i nie jest aktualnie używany do żadnej innej operacji powrotu po awarii.
- Masz stabilne połączenie z Internetem.
- Jest dostępny zarejestrowany nośnik startowy. Dodatkowe informacje można znaleźć w sekcji „Tworzenie nośników startowych do odzyskiwania systemów operacyjnych” w Podręczniku użytkownika programu Cyber Protection.
- Docelowy komputer fizyczny jest pierwotnym komputerem w lokalizacji lokalnej lub ma takie samo oprogramowanie układowe jak pierwotny komputer.
- Istnieje co najmniej jedna pełna kopia zapasowa maszyny wirtualnej w chmurze.

Aby wykonać powrót po awarii na komputer fizyczny

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Serwery**.
2. Wybierz serwer odzyskiwania znajdujący się w stanie **przełączania awaryjnego**.
3. Kliknij kartę **Powrót po awarii**.
4. W polu **Miejsce docelowe** wybierz **Komputer fizyczny**.

© Acronis International GmbH, 2003-2024

5. W polu **Docelowy nośnik startowy** kliknij **Określ**, wybierz nośnik startowy, a następnie kliknij **Gotowe**.

   Uwaga
   Zalecamy korzystanie z gotowych nośników startowych, ponieważ są one już skonfigurowane. Dodatkowe informacje można znaleźć w sekcji „Tworzenie nośników startowych do odzyskiwania systemów operacyjnych" w Podręczniku użytkownika programu Cyber Protection.

6. [Opcjonalnie] Aby zmienić domyślne mapowanie dysków, w polu **Mapowanie dysków** kliknij **Określ**, zamapuj dyski z kopii zapasowej na dyski komputera docelowego, a następnie kliknij **Gotowe**.
7. Kliknij **Rozpocznij przesyłanie danych**, a następnie w oknie potwierdzenia kliknij **Rozpocznij**.

   Uwaga
   Jeżeli w chmurze nie ma kopii zapasowej maszyny wirtualnej, system automatycznie wykona kopię zapasową przed fazą przesyłania danych.

   Rozpocznie się faza przesyłania danych. W konsoli będą wyświetlane następujące informacje:

Pole	Opis
Postęp	Ten parametr odzwierciedla ilość danych już przesłanych do lokalizacji lokalnej oraz całkowitą ilość danych do przesłania. Całkowita ilość danych obejmuje dane z ostatniej kopii zapasowej sprzed rozpoczęcia fazy przesyłania danych oraz kopie zapasowe nowo wygenerowanych danych (przyrosty kopii zapasowych), ponieważ maszyna wirtualna nadal działa podczas fazy przesyłania danych. Dlatego wartości parametru **Postęp** rosną w miarę upływu czasu. Ponieważ system używa technologii flashback podczas przesyłania danych i nie przesyła danych, które już są dostępne na komputerze docelowym, postęp może być szybszy niż ten, który został na początku obliczony przez konsolę.
Oszacowanie przestoju	Ten parametr wskazuje, jak długo maszyna wirtualna w chmurze będzie niedostępna w przypadku rozpoczęcia fazy przełączania w danej chwili. Wartość ta jest obliczana na podstawie wartości parametru **Postęp** i maleje w miarę upływu czasu. Ponieważ system używa technologii flashback podczas przesyłania danych i nie przesyła danych, które już są dostępne na komputerze docelowym, czas przestoju może być znacznie krótszy niż ten, który został na początku wyświetlony w konsoli.

8. Kliknij **Przełączanie**, a następnie w oknie potwierdzenia ponownie kliknij **Przełączanie**.

   Rozpocznie się faza przełączania. W konsoli będą wyświetlane następujące informacje:

© Acronis International GmbH, 2003-2024

Pole	Opis
Postęp	Ten parametr ilustruje postęp przywracania maszyny w lokalizacji lokalnej.
Szacowany czas do końca	Ten parametr ilustruje przybliżony czas zakończenia fazy przełączania, kiedy to będzie można włączyć komputer w lokalizacji lokalnej.

Uwaga
Jeśli do maszyny wirtualnej w chmurze nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, co spowoduje dłuższy przestój.

9. Po zakończeniu fazy **Przełączanie** uruchom ponownie nośnik startowy, a następnie sprawdź, czy komputer fizyczny w lokalizacji lokalnej działa zgodnie z oczekiwaniami.
   Dodatkowe informacje można znaleźć w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego" w Podręczniku użytkownika programu Cyber Protection.
10. Kliknij **Potwierdź powrót po awarii**, a następnie w oknie potwierdzenia kliknij **Potwierdź**, aby sfinalizować proces.
    Maszyna wirtualna w chmurze zostaje usunięta, a serwer odzyskiwania wraca do stanu **Stan gotowości**.

Uwaga
Zastosowanie planu ochrony na odzyskiwanym serwerze nie jest częścią procesu powrotu po awarii. Po zakończeniu procesu powrotu po awarii zastosuj plan ochrony na odzyskanym serwerze, aby wznowić jego ochronę. Możesz wykorzystać ten sam plan ochrony, który został zastosowany na pierwotnym serwerze, lub nowy plan ochrony z włączonym modułem **Odzyskiwanie po awarii**.

Ręczny powrót po awarii

Uwaga
Zalecamy korzystanie z ręcznego trybu powrotu po awarii tylko wtedy, gdy zaleci to zespół pomocy technicznej.

Proces powrotu po awarii można też uruchomić w trybie ręcznym. W takim przypadku przesłanie danych z kopii zapasowej w chmurze do lokalizacji lokalnej nie zostanie wykonane automatycznie. Trzeba to zrobić ręcznie po wyłączeniu maszyny wirtualnej w chmurze. Skutkuje to znacznym spowolnieniem procesu powrotu po awarii w trybie ręcznym i można się spodziewać dłuższego przestoju.

Proces powrotu po awarii w trybie ręcznym obejmuje następujące fazy:

1. **Planowanie**. W tej fazie jest przywracana infrastruktura IT w lokalizacji lokalnej (taka jak hosty i konfiguracje sieci), są konfigurowane parametry powrotu po awarii i jest planowany czas

© Acronis International GmbH, 2003-2024

rozpoczęcia przesyłania danych.

2. **Przełączanie**. W tej fazie jest wyłączana maszyna wirtualna w chmurze i tworzona kopia zapasowa nowo wygenerowanych danych. Jeśli na serwerze odzyskiwania nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, a to spowolni proces. Po utworzeniu kopii zapasowej należy ręcznie odzyskać komputer w lokalizacji lokalnej. Można odzyskać dysk przy użyciu nośnika startowego lub odzyskać cały komputer z kopii zapasowej w chmurze.
3. **Sprawdzanie poprawności**. W tej fazie należy sprawdzić, czy komputer fizyczny lub maszyna wirtualna w lokalizacji lokalnej działa poprawnie, i potwierdzić wykonanie powrotu po awarii. Po potwierdzeniu zostaje usunięta maszyna wirtualna w lokalizacji w chmurze, a serwer odzyskiwania wraca do stanu **Stan gotowości**.

Wykonywanie ręcznego powrotu po awarii

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Istnieje możliwość przeprowadzenia ręcznego powrotu po awarii na docelowy komputer fizyczny lub maszynę wirtualną w lokalizacji lokalnej.

Aby wykonać ręczny powrót po awarii

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Serwery**.
2. Wybierz serwer odzyskiwania znajdujący się w stanie **przełączania awaryjnego**.
3. Kliknij kartę **Powrót po awarii**.
4. W polu **Miejsce docelowe** wybierz **Komputer fizyczny**.
5. Kliknij ikonę koła zębatego, a następnie włącz przełącznik **Użyj trybu ręcznego**.
6. [Opcjonalnie] Oszacuj czas przestoju podczas procesu powrotu po awarii: podziel wartość **Rozmiar kopii zapasowej** przez wartość szybkości połączenia z Internetem.

   Uwaga
   W przypadku jednoczesnego wykonywania kilku procesów powrotu po awarii wartość szybkości połączenia z Internetem będzie mniejsza.

7. Kliknij **Przełączanie**, a następnie w oknie potwierdzenia ponownie kliknij **Przełączanie**.
   Maszyna wirtualna w lokalizacji w chmurze zostaje wyłączona.

   Uwaga
   Jeśli do maszyny wirtualnej w chmurze nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, co spowoduje dłuższy przestój.

8. Odzyskaj serwer z kopii zapasowej w chmurze na komputer fizyczny lub maszynę wirtualną w lokalizacji lokalnej. Dodatkowe informacje można znaleźć w sekcji „Odzyskiwanie komputera” w

© Acronis International GmbH, 2003-2024

Podręczniku użytkownika programu Cyber Protection.

9. Upewnij się, że proces odzyskiwania został ukończony i odzyskany komputer działa prawidłowo, a następnie kliknij **Przywrócono maszynę**.
10. Jeśli wszystko działa zgodnie z oczekiwaniami, kliknij **Potwierdź powrót po awarii**, a następnie w oknie potwierdzenia kliknij **Potwierdź**.

    Serwer odzyskiwania i punkty odzyskiwania będą gotowe do następnego przełączenia awaryjnego. Aby utworzyć nowe punkty odzyskiwania, zastosuj plan ochrony do nowego serwera lokalnego.

Uwaga
Zastosowanie planu ochrony na odzyskiwanym serwerze nie jest częścią procesu powrotu po awarii. Po zakończeniu procesu powrotu po awarii zastosuj plan ochrony na odzyskanym serwerze, aby wznowić jego ochronę. Możesz wykorzystać ten sam plan ochrony, który został zastosowany na pierwotnym serwerze, lub nowy plan ochrony z włączonym modułem **Odzyskiwanie po awarii**.

Praca z zaszyfrowanymi kopiami zapasowymi

Istnieje możliwość tworzenia serwerów odzyskiwania z zaszyfrowanych kopii zapasowych. Dla wygody można skonfigurować automatyczne stosowanie hasła do zaszyfrowanej kopii zapasowej podczas przełączania awaryjnego na serwer odzyskiwania.

Tworząc serwer odzyskiwania, można podać hasło, które ma być używane do automatycznych operacji odzyskiwania po awarii. Zostanie ono zapisane w Magazynie poświadczeń, bezpiecznym repozytorium poświadczeń dostępnym w sekcji **Ustawienia** > **Poświadczenia**.

Jedno poświadczenie można powiązać z kilkoma kopiami zapasowymi.

Aby zarządzać hasłami zapisanymi w Magazynie poświadczeń

1. Przejdź do sekcji **Ustawienia** > **Poświadczenia**.
2. Aby zarządzać określonym poświadczeniem, kliknij ikonę w ostatniej kolumnie. Możesz wyświetlić elementy powiązane z tym poświadczeniem.
   - Aby usunąć powiązanie kopii zapasowej z wybranym poświadczeniem, kliknij ikonę kosza obok tej kopii. W rezultacie podczas przełączania awaryjnego na serwer odzyskiwania hasło trzeba będzie podać ręcznie.
   - Aby edytować poświadczenie, kliknij **Edytuj** i określ nazwę użytkownika lub hasło.
   - Aby usunąć poświadczenie, kliknij **Usuń**. Uwaga: podczas przełączania awaryjnego na serwer odzyskiwania hasło trzeba będzie podać ręcznie.

© Acronis International GmbH, 2003-2024

Operacje dotyczące maszyn wirtualnych Microsoft Azure

Uwaga
Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Można przeprowadzić przełączanie awaryjne maszyn wirtualnych Microsoft Azure na środowisko Acronis Cyber Protect Cloud. Aby uzyskać więcej informacji, zobacz "Wykonywanie przełączenia awaryjnego" (s. 844).

Potem można wykonać powrót po awarii ze środowiska Acronis Cyber Protect Cloud z powrotem na maszyny wirtualne Azure. Ten proces powrotu po awarii wygląda tak samo jak powrót po awarii na komputer fizyczny. Aby uzyskać więcej informacji, zobacz "Wymagania wstępne" (s. 854).

Uwaga
Aby zarejestrować nową maszynę wirtualną Azure w celu wykonania powrotu po awarii, można użyć rozszerzenia Acronis Backup VM dostępnego na platformie Azure.

Można skonfigurować połączenie IPsec VPN multi-site między środowiskiem Acronis Cyber Protect Cloud a bramą VPN Azure. Aby uzyskać więcej informacji, zobacz "Konfigurowanie połączenia IPsec VPN multi-site" (s. 810).

Konfigurowanie serwerów podstawowych

W tej sekcji opisano, jak można utworzyć serwery podstawowe i nimi zarządzać.

Tworzenie serwera podstawowego

Wymagania wstępne

- Trzeba ustawić typ łączności z lokalizacją w chmurze.

Aby utworzyć serwer podstawowy

1. Przejdź do karty **Odzyskiwanie po awarii** > **Serwery** > **Serwery podstawowe**.
2. Kliknij **Utwórz**.
3. Wybierz szablon dla nowej maszyny wirtualnej.
4. Wybierz wariant konfiguracji (liczbę rdzeni wirtualnych i wielkość pamięci RAM). W poniższej tabeli przedstawiono maksymalną łączną ilość miejsca na dysku (GB) w przypadku każdego wariantu.

Typ	vCPU	RAM (GB)	Maksymalna łączna ilość miejsca na dysku (GB)
W1	1	2	500

© Acronis International GmbH, 2003-2024

Typ	vCPU	RAM (GB)	Maksymalna łączna ilość miejsca na dysku (GB)
F2	1	4	1000
W3	2	8	2000
W4	4	16	4000
W5	8	32	8000
W6	16	64	16000
W7	16	128	32000
W8	16	256	64000

Uwaga
Podano liczbę punktów obliczeniowych wykorzystywanych w przypadku każdej opcji. Liczba punktów obliczeniowych odzwierciedla koszt działania serwera podstawowego przez godzinę. Aby uzyskać więcej informacji, zobacz "Punkty obliczeniowe" (s. 791).

5. [Opcjonalnie] Zmień rozmiar dysku wirtualnego. Jeśli potrzebujesz więcej niż jednego dysku twardego, kliknij **Dodaj dysk**, a następnie określ rozmiar nowego dysku. Obecnie można dodać maksymalnie 10 dysków serwera podstawowego.
6. Wskaż sieć w chmurze, do której będzie należeć serwer podstawowy.
7. Wybierz **DHCP**.

Opcja DHCP	Opis
Dostępne w lokalizacji w chmurze	Ustawienie domyślne. Adres IP serwera zostanie udostępniony przez automatycznie skonfigurowany serwer DHCP w chmurze.
Niestandardowe	Adres IP serwera zostanie udostępniony przez Twój własny serwer DHCP w chmurze.

8. [Opcjonalnie] Podaj **adres MAC**.
   Adres MAC jest unikatowym identyfikatorem przypisanym do karty sieciowej serwera. W przypadku korzystania z niestandardowego serwera DHCP można go skonfigurować tak, aby zawsze przypisywał określone adresy IP do określonych adresów MAC. Dzięki temu serwer podstawowy zawsze otrzymuje ten sam adres IP. Można uruchamiać aplikacje, które mają licencje zarejestrowane na adres MAC.
9. Określ adres IP, który będzie znajdował się w sieci produkcyjnej serwera. Domyślnie wybierany jest pierwszy niezajęty adres IP w Twojej sieci produkcyjnej.

© Acronis International GmbH, 2003-2024

Uwaga
Jeśli korzystasz z serwera DHCP, dodaj ten adres IP do listy elementów wykluczonych serwera, aby uniknąć konfliktu adresów IP.
W przypadku korzystania z niestandardowego serwera DHCP trzeba w polu **Adres IP w sieci produkcyjnej** podać ten sam adres, który został skonfigurowany na serwerze DHCP. W przeciwnym razie testowe przełączanie awaryjne nie będzie działać prawidłowo i nie będzie można się komunikować z serwerem przy użyciu publicznego adresu IP.

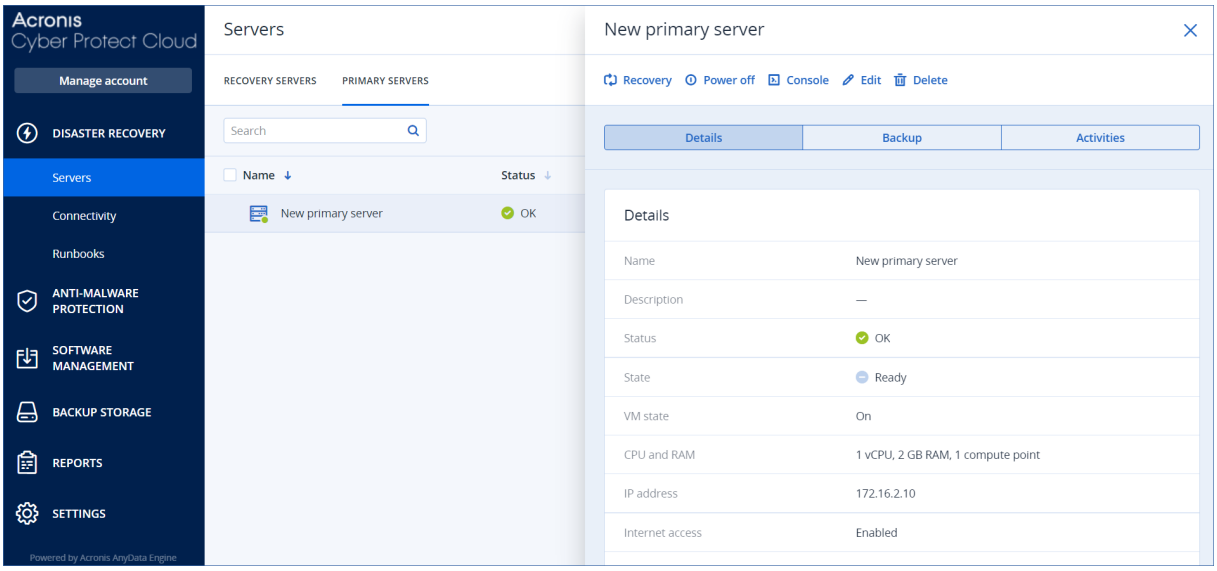
10. [Opcjonalnie] Zaznacz pole wyboru **Dostęp do Internetu**.
    Opcja ta pozwala serwerowi podstawowemu na dostęp do Internetu. Domyślnie port TCP 25 jest otwarty dla połączeń wychodzących do publicznych adresów IP.
11. [Opcjonalnie] Zaznacz pole wyboru **Użyj publicznego adresu IP**.
    Publiczny adres IP serwera podstawowego umożliwia uzyskiwanie do niego dostępu z Internetu. Jeśli pole wyboru pozostanie niezaznaczone, serwer będzie dostępny wyłącznie w Twojej sieci produkcyjnej.
    Publiczny adres IP zostanie wyświetlony po zakończeniu konfiguracji. Domyślnie port TCP 443 jest otwarty dla połączeń przychodzących do publicznych adresów IP.

    Uwaga
    Jeśli wyczyścisz pole wyboru **Użyj publicznego adresu IP** lub usuniesz serwer odzyskiwania, jego publiczny adres IP nie zostanie zastrzeżony.

12. [Opcjonalnie] Wybierz **Ustaw próg RPO**.
    Próg RPO określa maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania a czasem bieżącym. Można ustawić wartość z przedziałów: 15– 60 minut, 1–24 godz., 1–14 dni.
13. Podaj nazwę serwera podstawowego.
14. [Opcjonalnie] Podaj opis serwera podstawowego.
15. [Opcjonalnie] Kliknij kartę **Reguły zapory chmury**, aby edytować domyślne reguły zapory. Aby uzyskać więcej informacji, zobacz "Ustawianie reguł zapory dla serwerów chmurowych" (s. 864).
16. Kliknij **Utwórz**.

Serwer podstawowy zostanie udostępniony w sieci produkcyjnej. Możesz zarządzać serwerem za pomocą jego konsoli, funkcji RDP, połączenia SSH lub programu TeamViewer.

© Acronis International GmbH, 2003-2024



Działania na serwerze podstawowym

Serwer podstawowy pojawi się na karcie **Odzyskiwanie po awarii** > **Serwery** > **Serwery podstawowe** w konsoli Cyber Protect.

Aby uruchomić lub zatrzymać serwer, kliknij **Włącz** lub **Wyłącz** na panelu serwera podstawowego.

Aby edytować ustawienia serwera podstawowego, zatrzymaj serwer, a następnie kliknij **Edytuj**.

Aby zastosować plan ochrony do serwera podstawowego, zaznacz go i na karcie **Plan** kliknij **Utwórz**. Zostanie wyświetlony wstępnie zdefiniowany plan ochrony, w którym możesz zmienić tylko harmonogram oraz reguły przechowywania. Aby uzyskać więcej informacji, zobacz sekcję „Tworzenie kopii zapasowych serwerów chmurowych”.

Zarządzanie serwerami chmurowymi

Aby zarządzać serwerami chmurowymi, wybierz **Odzyskiwanie po awarii** >**Serwery**. Są tam dostępne dwie karty: **Serwery odzyskiwania** i **Serwery podstawowe**. Aby wyświetlić wszystkie opcjonalne kolumny w tabeli, kliknij ikonę koła zębatego.

Zaznaczając serwer chmurowy, można wyświetlić następujące informacje na jego temat.

Nazwa kolumny	Opis
Nazwa	Zdefiniowana przez Ciebie nazwa serwera chmurowego
Status	Status odzwierciedlający największy problem z danym serwerem chmurowym (na podstawie aktywnych alertów)
Stan	Stan serwera chmurowego
Stan maszyny wirtualnej	Stan zasilania maszyny wirtualnej powiązanej z serwerem chmurowym

© Acronis International GmbH, 2003-2024

Aktywna lokalizacja	Lokalizacja, w której jest hostowany serwer chmurowy. Na przykład **Chmura**.
Próg RPO	Maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania nadającym się do wykorzystania do przełączenia awaryjnego a czasem bieżącym. Dopuszczalne są wartości z następujących przedziałów: 15–60 minut, 1–24 godz., 1–14 dni.
Zgodność z wymogami RPO	Zgodność z wymogami RPO to stosunek między rzeczywistym wskaźnikiem RPO a progiem RPO. Zgodność z wymogami RPO jest pokazywana tylko wtedy, gdy został zdefiniowany próg RPO. Oblicza się ją następująco: **Zgodność z wymogami RPO = rzeczywisty wskaźnik RPO / próg RPO** gdzie **Rzeczywisty wskaźnik RPO = czas bieżący – czas ostatniego punktu odzyskiwania** **Statusy zgodności z wymogami RPO** Zależnie od wartości wskaźnika stosunku rzeczywistego wskaźnika RPO do progu RPO używane są następujące statusy: • **Zgodność**. Zgodność z wymogami RPO < 1x. Serwer mieści się w progu RPO. • **Przekroczenie**. Zgodność z wymogami RPO <= 2x. Serwer narusza próg RPO. • **Znaczne przekroczenie**. Zgodność z wymogami RPO <= 4x. Serwer ponad dwukrotnie przekracza próg RPO. • **Krytyczne przekroczenie**. Zgodność z wymogami RPO > 4x. Serwer ponad czterokrotnie przekracza próg RPO. • **Oczekujące (brak kopii zapasowych)**. Serwer jest chroniony przy użyciu planu ochrony, ale kopia zapasowa dopiero jest tworzona i nie została jeszcze ukończona.
Rzeczywisty wskaźnik RPO	Czas, jaki upłynął od utworzenia ostatniego punktu odzyskiwania
Ostatni punkt odzyskiwania	Data i godzina utworzenia ostatniego punktu odzyskiwania

Reguły zapory dotyczące serwerów chmurowych

Reguły zapory można skonfigurować tak, aby kontrolować ruch przychodzący i wychodzący serwera podstawowego oraz serwera odzyskiwania w lokalizacji w chmurze.

Reguły dotyczące połączeń przychodzących można skonfigurować po przydzieleniu serwerowi chmurowego publicznego adresu IP. Domyślnie dozwolony jest port TCP 443, a w przypadku pozostałych połączeń przychodzących jest aktywna odmowa dostępu. Można zmienić domyślne reguły zapory sieciowej oraz dodać lub usunąć wyjątki dotyczące połączeń przychodzących. Jeśli

© Acronis International GmbH, 2003-2024

publiczny adres IP nie zostanie przydzielony, można jedynie przeglądać reguły dotyczące połączeń przychodzących, ale nie można ich konfigurować.

Reguły dotyczące połączeń wychodzących można skonfigurować po przydzieleniu serwerowi chmurowego dostępu do Internetu. Domyślnie skonfigurowana jest odmowa dostępu w przypadku portu TCP 25, a pozostałe połączenia wychodzące są dozwolone. Można zmienić domyślne reguły zapory sieciowej oraz dodać lub usunąć wyjątki dotyczące połączeń wychodzących. Jeśli dostęp do Internetu nie zostanie przydzielony, można jedynie przeglądać reguły dotyczące połączeń wychodzących, ale nie można ich konfigurować.

Uwaga
Ze względów bezpieczeństwa istnieją pewne gotowe reguły zapory, których nie można zmienić.

W przypadku połączeń przychodzących i wychodzących:

- Zezwolenie na obsługę poleceń ping: ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Permit ICMP need-to-frag (type 3, code 4)
- Permit TTL exceeded (type 11, code 0)

Tylko w przypadku połączeń przychodzących:

- Część, której nie można konfigurować: Odmawiaj w przypadku wszystkich

Tylko w przypadku połączeń wychodzących:

- Część, której nie można konfigurować: Odrzucaj wszystkie

Ustawianie reguł zapory dla serwerów chmurowych

Istnieje możliwość edycji domyślnych reguł zapory dla serwera podstawowego i serwera odzyskiwania w chmurze.

Aby edytować reguły zapory serwera w lokalizacji w chmurze

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Serwery**.
2. Jeśli chcesz edytować reguły zapory serwera odzyskiwania, kliknij kartę **Serwery odzyskiwania**.Jeśli zaś chcesz edytować reguły zapory serwera podstawowego, kliknij kartę **Serwery podstawowe**.
3. Kliknij serwer, a następnie kliknij **Edytuj**.
4. Kliknij kartę **Reguły zapory chmury**.
5. Jeśli chcesz zmienić czynność domyślną dotyczącą połączeń przychodzących:

© Acronis International GmbH, 2003-2024

a. W polu rozwijanym **Przychodzące** wybierz czynność domyślną.

Czynność	Opis
Odmawiaj w przypadku wszystkich	Powoduje odmowę obsługi ruchu przychodzącego. Można dodawać wyjątki i zezwalać na ruch z określonych adresów IP, protokołów i portów.
Zezwalaj w przypadku wszystkich	Umożliwia zezwolenie na cały przychodzący ruch TCP i UDP. Można dodawać wyjątki i odmawiać obsługi ruchu z określonych adresów IP, protokołów i portów.

Uwaga
Zmiana czynności domyślnej powoduje unieważnienie i usunięcie konfiguracji istniejących reguł dotyczących połączeń przychodzących.

b. [Opcjonalnie] Jeśli chcesz zapisać już dodane wyjątki, w oknie potwierdzenia wybierz **Zapisz wypełnione wyjątki**.

c. Kliknij **Potwierdź**.

6. Jeśli chcesz dodać wyjątek:

a. Kliknij **Dodaj wyjątek**.

b. Określ parametry zapory.

Parametr zapory	Opis
Protokół	Wybierz protokół połączenia. Obsługiwane są następujące opcje: • **TCP** • **UDP** • **TCP+UDP**
Port serwera	Wybierz porty, których dotyczy reguła. Możesz określić: • Konkretny numer portu (na przykład `2298`) • Zakres numerów portów (na przykład `6000-6700`) • Dowolny numer portu Użyj symbolu `*`, jeśli reguła ma dotyczyć każdego numeru portu.
Adres IP klienta	Wybierz adresy IP, których dotyczy reguła. Możesz określić: • Konkretny adres IP (na przykład `192.168.0.0`) • Zakres adresów IP w notacji CIDR (na przykład `192.168.0.0/24`) • Dowolny adres IP Użyj symbolu `*`, jeśli reguła ma dotyczyć każdego adresu IP.

7. Jeśli chcesz usunąć jakiś wyjątek dotyczący połączeń przychodzących, kliknij znajdującą się obok niego ikonę kosza.
8. Jeśli chcesz zmienić czynność domyślną dotyczącą połączeń wychodzących:

© Acronis International GmbH, 2003-2024

a. W polu rozwijanym **Wychodzące** wybierz czynność domyślną.

Czynność	Opis
Odmawiaj w przypadku wszystkich	Powoduje odmowę obsługi ruchu wychodzącego. Można dodawać wyjątki i zezwalać na ruch do określonych adresów IP, protokołów i portów.
Zezwalaj w przypadku wszystkich	Powoduje zezwolenie na wszelki ruch wychodzący. Można dodawać wyjątki i odmawiać obsługi ruchu z określonych adresów IP, protokołów i portów.

Uwaga
Zmiana czynności domyślnej powoduje unieważnienie i usunięcie konfiguracji istniejących reguł dotyczących połączeń wychodzących.

b. [Opcjonalnie] Jeśli chcesz zapisać już dodane wyjątki, w oknie potwierdzenia wybierz **Zapisz wypełnione wyjątki**.

c. Kliknij **Potwierdź**.

9. Jeśli chcesz dodać wyjątek:

a. Kliknij **Dodaj wyjątek**.

b. Określ parametry zapory.

Parametr zapory	Opis
Protokół	Wybierz protokół połączenia. Obsługiwane są następujące opcje: • **TCP** • **UDP** • **TCP+UDP**
Port serwera	Wybierz porty, których dotyczy reguła. Możesz określić: • Konkretny numer portu (na przykład `2298`) • Zakres numerów portów (na przykład `6000-6700`) • Dowolny numer portu Użyj symbolu `*`, jeśli reguła ma dotyczyć każdego numeru portu.
Adres IP klienta	Wybierz adresy IP, których dotyczy reguła. Możesz określić: • Konkretny adres IP (na przykład `192.168.0.0`) • Zakres adresów IP w notacji CIDR (na przykład `192.168.0.0/24`) • Dowolny adres IP Użyj symbolu `*`, jeśli reguła ma dotyczyć każdego adresu IP.

10. Jeśli chcesz usunąć jakiś wyjątek dotyczący połączeń wychodzących, kliknij znajdującą się obok niego ikonę kosza.
11. Kliknij **Zapisz**.

© Acronis International GmbH, 2003-2024

Sprawdzanie działań dotyczących zapory chmury

Po zaktualizowaniu konfiguracji reguł zapory serwera chmurowego w konsoli Cyber Protect będzie dostępny dziennik działań dotyczących aktualizacji. Można przejrzeć dziennik i sprawdzić takie informacje jak:

- nazwa użytkownika, który zaktualizował konfigurację
- data i godzina aktualizacji
- ustawienia zapory dla połączeń przychodzących i wychodzących
- domyślne czynności dotyczące połączeń przychodzących i wychodzących
- protokoły, porty i adresy IP wyjątków dotyczących połączeń przychodzących i wychodzących

Aby wyświetlić szczegóły zmian konfiguracji reguł zapory chmury

1. W konsoli Cyber Protect kliknij **Monitorowanie** > **Działania**.
2. Kliknij odpowiednie działanie, a następnie kliknij **Wszystkie właściwości**.
   Działanie powinno być opisane jako **Aktualizowanie konfiguracji serwera w chmurze**.
3. W polu **kontekst** sprawdź interesujące Cię informacje.

Tworzenie kopii zapasowych serwerów chmurowych

Kopie zapasowe serwerów podstawowych i serwerów odzyskiwania są tworzone bezagentowo w chmurze. Te kopie zapasowe mają następujące ograniczenia.

- Jedyną możliwą lokalizacją kopii zapasowej jest chmura. Kopie zapasowe serwerów podstawowych są tworzone w magazynie **Kopia zapasowa serwerów podstawowych**.

  Uwaga
  Lokalizacje kopii zapasowych na platformie Microsoft Azure nie są obsługiwane.

- Nie można zastosować jednego planu tworzenia kopii zapasowych do wielu serwerów. Każdy serwer musi mieć własny plan tworzenia kopii zapasowych, nawet jeśli wszystkie te plany mają takie same ustawienia.
- Do serwera można zastosować tylko jeden plan tworzenia kopii zapasowych.
- Tworzenie kopii zapasowych uwzględniające aplikacje nie jest obsługiwane.
- Szyfrowanie jest niedostępne.
- Opcje tworzenia kopii zapasowych są niedostępne.

W wyniku usunięcie serwera podstawowego zostają usunięte również jego kopie zapasowe.

Kopia zapasowa serwera odzyskiwania jest tworzona tylko w stanie przełączania awaryjnego. Kopie zapasowe serwera odzyskiwania kontynuują tworzenie kopii zapasowych zgodnie z pierwotną

© Acronis International GmbH, 2003-2024

kolejnością. W razie wykonania powrotu po awarii pierwotny serwer może kontynuować tę sekwencję tworzenia kopii zapasowych. Kopie zapasowe serwera odzyskiwania można zatem usuwać ręcznie lub poprzez zastosowanie reguł przechowywania. Kopie zapasowe serwera odzyskiwania są zawsze zachowywane po jego usunięciu.

Uwaga
Plany tworzenia kopii zapasowych dotyczące serwerów chmurowych są wykonywane według czasu UTC.

Orkiestracja (runbooki)

Uwaga
Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Runbook to zestaw instrukcji opisujących sposób uruchamiania środowiska produkcyjnego w chmurze. Runbooki można tworzyć z poziomu konsoli Cyber Protect. Aby otworzyć ekran **Runbooki**, wybierz **Odzyskiwanie po awarii** > **Runbooki**.

Dlaczego warto korzystać z runbooków?

Za pomocą runbooków można:

- Automatyzację przełączania awaryjnego jednego lub wielu serwerów
- Automatyczne sprawdzanie wyników operacji przełączania awaryjnego przez wysłanie sondy ping na adres IP serwera i sprawdzanie połączenia określonego portu
- Określanie sekwencji operacji dla serwerów z uruchomionymi aplikacjami rozproszonymi
- Uwzględnienie czynności manualnych w toku pracy
- Weryfikację integralności stosowanego rozwiązania do odzyskiwania po awarii przez uruchomienie runbooków w trybie testowania

Tworzenie runbooka

Runbook składa się z wykonywanych kolejno kroków. Krok składa się z rozpoczynanych jednocześnie czynności.

Możesz postąpić zgodnie z poniższą instrukcją lub obejrzeć instruktaż wideo.

Aby utworzyć runbook

1. W konsoli Cyber Protection przejdź do sekcji **Odzyskiwanie po awarii** > **Runbooki**.
2. Kliknij **Utwórz runbook**.
3. Kliknij **Dodaj krok**.
4. Kliknij **Dodaj czynność**, a następnie wybierz czynność, którą chcesz dodać do kroku.

© Acronis International GmbH, 2003-2024

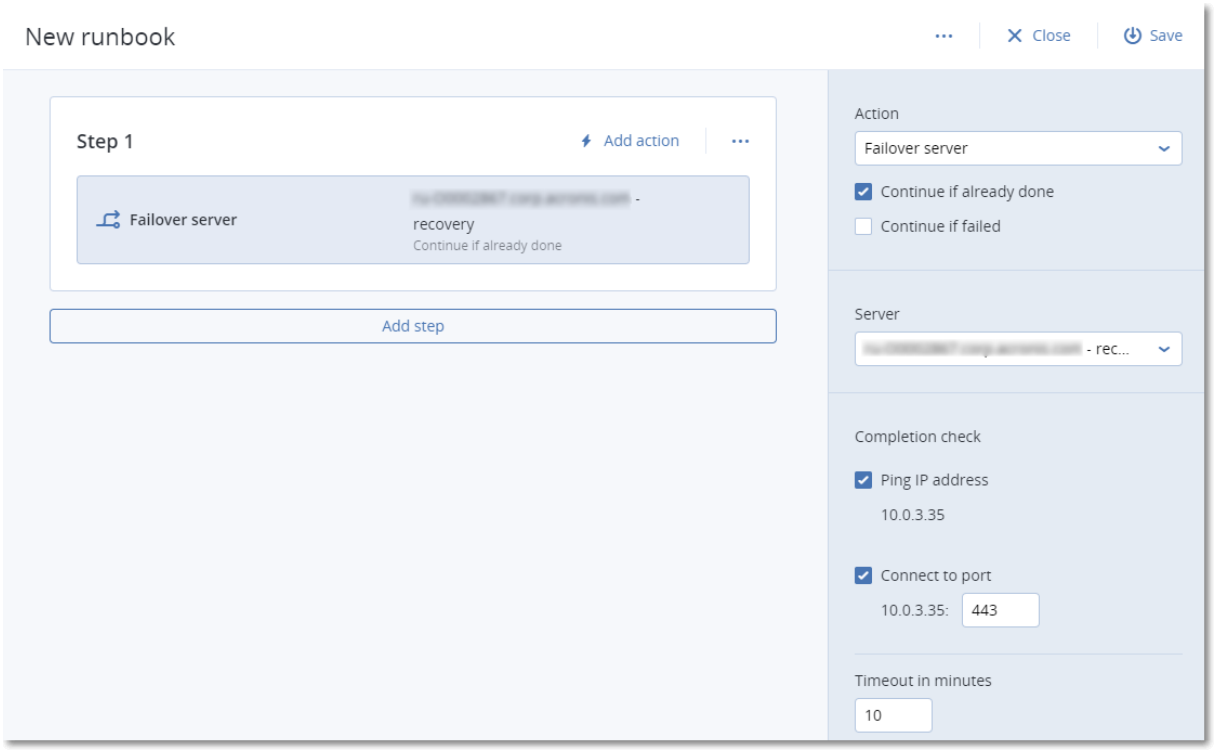
Czynność	Opis
Przełączenie awaryjne serwera	Wykonuje przełączanie awaryjne serwera chmurowego. Aby zdefiniować tę czynność, trzeba wybrać serwer chmurowy i skonfigurować dostępne dla danej czynności parametry runbooka. Aby uzyskać więcej informacji na temat tych parametrów, zobacz sekcję "Parametry runbooka" (s. 871). **Uwaga** Jeśli wybrana kopia zapasowa serwera jest zaszyfrowana za pomocą szyfrowania jako właściwość komputera, czynność **Przełączenie awaryjne serwera** zostanie wstrzymana i automatycznie zmieniona na **Wymagane działanie**. Aby kontynuować wykonywanie runbooka, musisz podać hasło do zaszyfrowanej kopii zapasowej.
Wykonaj powrót po awarii serwera	Przeprowadza powrót po awarii serwera chmurowego. Aby zdefiniować to działanie, musisz wybrać serwer chmurowy i skonfigurować dostępne dla tego działania parametry runbooka. Aby uzyskać więcej informacji na temat tych ustawień, zobacz sekcję "Parametry runbooka" (s. 871). **Uwaga** W przypadku wykonywania operacji przy użyciu runbooków jest obsługiwany tylko ręczny tryb powrotu po awarii. Oznacza to, że po rozpoczęciu powrotu po awarii przez wykonanie runbooka obejmującego krok **Wykonaj powrót po awarii serwera** procedura będzie wymagała ręcznych interakcji: trzeba będzie ręcznie odzyskać komputer, a następnie potwierdzić lub anulować proces powrotu po awarii na karcie **Odzyskiwanie po awarii** > **Serwery**.
Uruchom serwer	Uruchamia serwer chmurowy. Aby zdefiniować to działanie, musisz wybrać serwer chmurowy i skonfigurować dostępne w przypadku tej czynności parametry runbooka. Aby uzyskać więcej informacji na temat tych ustawień, zobacz sekcję "Parametry runbooka" (s. 871). **Uwaga** Czynność **Uruchom serwer** nie może być stosowana w przypadku operacji testowego przełączania awaryjnego w runbookach. Jeśli spróbujesz wykonać taką czynność, zakończy się ona niepowodzeniem z następującym komunikatem o błędzie: Niepowodzenie: Czynność nie ma zastosowania w bieżącym stanie serwera.
Zatrzymaj serwer	Zatrzymuje serwer chmurowy. Aby zdefiniować tę czynność, musisz wybrać serwer chmurowy i skonfigurować dostępne w przypadku tej czynności parametry runbooka. Aby uzyskać więcej informacji na temat tych ustawień, zobacz sekcję "Parametry runbooka" (s. 871).

© Acronis International GmbH, 2003-2024

Czynność	Opis
	Uwaga Czynność **Zatrzymaj serwer** nie może być stosowana w przypadku operacji testowego przełączania awaryjnego w runbookach. Jeśli spróbujesz wykonać taką czynność, zakończy się ona niepowodzeniem z następującym komunikatem o błędzie: Niepowodzenie: Czynność nie ma zastosowania w bieżącym stanie serwera.
Operacja ręczna	Operacja ręczna wymaga działań ze strony użytkownika. Aby zdefiniować tę czynność, trzeba wprowadzić opis. Gdy sekwencja runbooka dojdzie do operacji ręcznej, runbook zostanie wstrzymany i nie będzie kontynuowany, dopóki użytkownik nie wykona wymaganej operacji ręcznej, na przykład nie kliknie przycisku potwierdzenia.
Wykonaj runbook	Powoduje wykonanie kolejnego runbooka. Aby zdefiniować tę czynność, musisz wybrać runbook. Runbook może zawierać tylko jedno wykonanie danego runbooka. Na przykład jeśli dodałeś czynność "wykonaj Runbook A", możesz dodać czynność "wykonaj Runbook B", ale nie możesz dodać kolejnej czynności "wykonaj Runbook A".

5. Zdefiniuj parametry runbooka na potrzeby danej czynności. Aby uzyskać więcej informacji na temat tych parametrów, zobacz sekcję "Parametry runbooka" (s. 871).
6. [Opcjonalnie] Aby dodać opis kroku:
   a. Kliknij ikonę wielokropka, a następnie kliknij **Opis**.
   b. Wprowadź opis kroku.
   c. Kliknij **Gotowe**.
7. Powtarzaj kroki 3–6, dopóki nie utworzysz pożądanej sekwencji kroków i czynności.
8. [Opcjonalnie] Aby zmienić domyślną nazwę runbooka:
   a. Kliknij ikonę wielokropka.
   b. Wprowadź nazwę runbooka.
   c. Wprowadź opis runbooka.
   d. Kliknij **Gotowe**.
9. Kliknij **Zapisz**.
10. Kliknij **Zamknij**.

© Acronis International GmbH, 2003-2024



Parametry runbooka

Parametry runbooka to specyficzne ustawienia, które trzeba skonfigurować, aby zdefiniować działanie runbooka. Istnieją dwie kategorie parametrów runbooka — parametry czynności i parametry sprawdzania ukończenia.

Parametry czynności definiują zachowanie runbooka w zależności od początkowego stanu lub wyniku czynności.

Parametry sprawdzania ukończenia zapewniają, że serwer jest dostępny i świadczy niezbędne usługi. Jeśli sprawdzenie ukończenia się nie powiedzie, czynność jest uznawana za zakończoną niepowodzeniem.

W poniższej tabeli opisano konfigurowalne parametry runbooka dla każdej czynności.

Parametr runbooka	Kategoria	Dostępny na potrzeby czynności	Opis
Kontynuuj, jeśli już wykonano	Parametr czynności	• **Przełączenie awaryjne serwera** • **Uruchom serwer** • **Zatrzymaj serwer** • **Wykonaj powrót po awarii serwera**	Ten parametr definiuje zachowanie runbooka, gdy żądana czynność jest już wykonana (na przykład przełączanie awaryjne zostało już przeprowadzone lub serwer już działa). Włączenie tego parametru oznacza, że runbook wyśle ostrzeżenie i będzie kontynuował działanie. Wyłączenie tego parametru oznacza, że czynność się nie powiedzie, a wówczas runbook również przestanie

© Acronis International GmbH, 2003-2024

Parametr runbooka	Kategoria	Dostępny na potrzeby czynności	Opis
			działać. Domyślnie ten parametr jest włączony.
Kontynuuj, jeśli czynność się nie powiodła	Parametr czynności	• **Przełączenie awaryjne serwera** • **Uruchom serwer** • **Zatrzymaj serwer** • **Wykonaj powrót po awarii serwera**	Ten parametr definiuje zachowanie runbooka, gdy żądana czynność się nie powiedzie. Włączenie tego parametru oznacza, że runbook wyśle ostrzeżenie i będzie kontynuował czynność. Wyłączenie tego parametru oznacza, że czynność się nie powiedzie, a wówczas runbook również przestanie działać. Domyślnie ten parametr jest wyłączony.
Wysyłanie sondy ping na adres IP	Kontrola ukończenia	• **Uruchom serwer**	Oprogramowanie będzie wysyłać sondę ping na produkcyjny adres IP serwera w chmurze, dopóki serwer nie odpowie lub nie zostanie przekroczony limit czasu, w zależności od tego, które z tych zdarzeń nastąpi jako pierwsze.
Połącz z portem (domyślnie 443)	Kontrola ukończenia	• **Przełączenie awaryjne serwera** • **Uruchom serwer**	Oprogramowanie będzie próbować połączyć się z serwerem w chmurze, korzystając z produkcyjnego adresu IP oraz wskazanego portu, dopóki połączenie nie zostanie nawiązane lub nie zostanie przekroczony limit czasu, w zależności od tego, które z tych zdarzeń nastąpi jako pierwsze. W ten sposób możesz sprawdzić, czy aplikacja nasłuchująca dany port działa.
Limit czasu w minutach	Kontrola ukończenia	• **Przełączenie awaryjne serwera** • **Uruchom serwer**	Domyślny limit czasu wynosi 10 minut.

Operacje przy użyciu runbooków

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Aby uzyskać dostęp do listy operacji, najedź kursorem na runbook i kliknij ikonę wielokropka. Gdy runbook nie działa, dostępne są następujące operacje:

© Acronis International GmbH, 2003-2024

- **Wykonaj**
- **Edytuj**
- **Klonuj**
- **Usuń**

Wykonywanie runbooka

Za każdym razem gdy klikniesz **Wykonaj**, wyświetlona zostanie prośba o podanie parametrów wykonania. Parametry te będą zastosowane do wszystkich operacji przełączania awaryjnego i powrotu po awarii zawartych w runbooku. Runbooki wyszczególnione w operacjach **Wykonaj runbook** dziedziczą te parametry z głównego runbooka.

- **Tryb przełączania awaryjnego i powrotu po awarii**
  Wybierz, czy chcesz wykonać testowe przełączanie awaryjne (domyślnie) czy prawdziwe (produkcyjne) przełączanie awaryjne. Tryb przywracania po awarii będzie powiązany z wybranym trybem przełączania awaryjnego.
- **Punkt odzyskiwania po awarii**
  Wybierz ostatni punkt odzyskiwania (domyślnie) lub wybierz żądany punkt w przeszłości. W tym drugim przypadku dla każdego serwera zostaną wybrane punkty odzyskiwania stworzone najbliżej przed określoną datą i godziną.

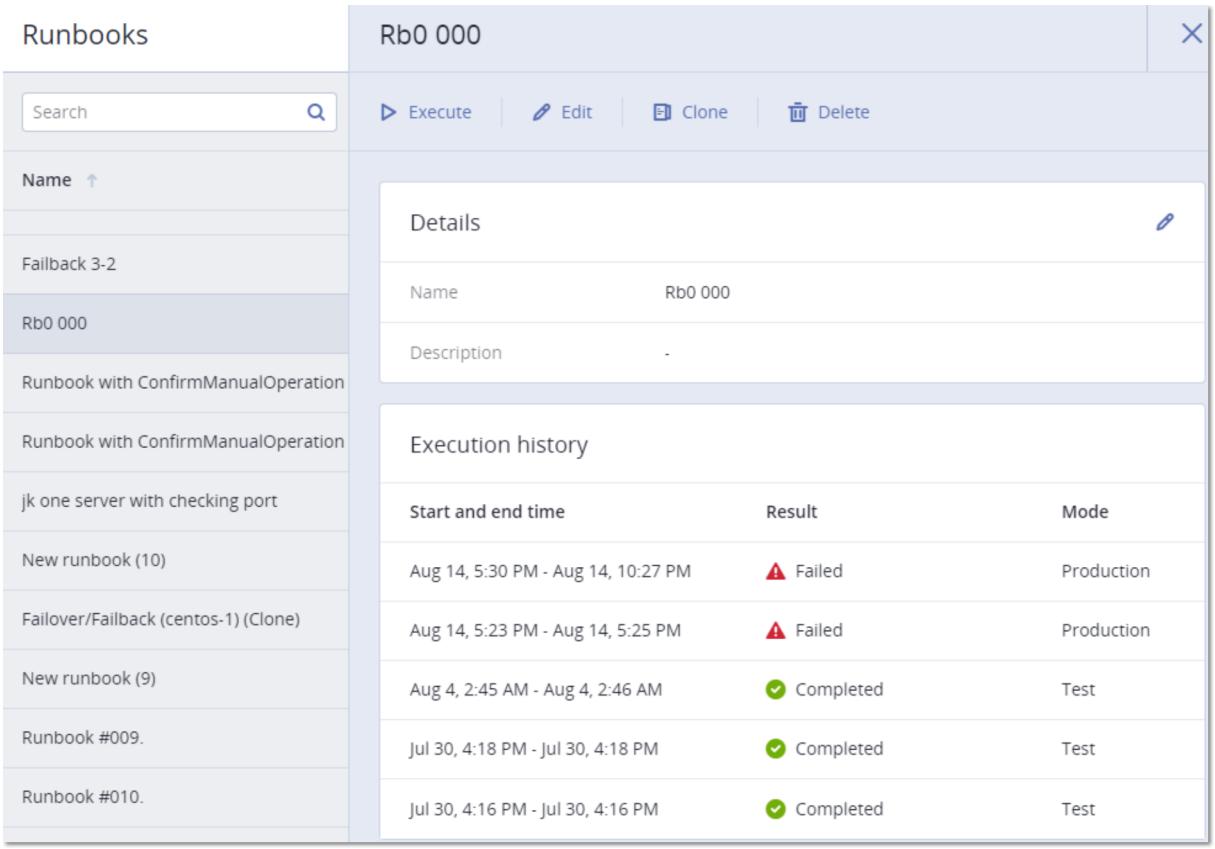
Zatrzymywanie wykonywania runbooka

Podczas wykonywania runbooka możesz na liście operacji wybrać pozycję **Stop**. Oprogramowanie dokończy wszystkie rozpoczęte działania z wyjątkiem tych, które wymagają działania użytkownika.

Wyświetlanie historii wykonania

Gdy na karcie **Runbooki** wybierzesz runbooka, oprogramowanie wyświetli szczegóły na jego temat oraz historię wykonania. Kliknij wiersz odpowiadający konkretnemu wykonaniu, aby wyświetlić jego dziennik.

© Acronis International GmbH, 2003-2024



© Acronis International GmbH, 2003-2024

Konfigurowanie ochrony przed wirusami i złośliwym oprogramowaniem

Uwaga
Na komputerach z systemem Windows funkcja ochrony przed złośliwym oprogramowaniem wymaga instalacji agenta dla usługi Ochrona przed złośliwym oprogramowaniem, a funkcja filtrowania adresów URL wymaga instalacji agenta dla usługi Filtrowanie adresów URL. Agenty te są instalowane automatycznie w przypadku chronionych maszyn, jeśli w ich planach ochrony włączono moduł **Ochrona przed wirusami i złośliwym oprogramowaniem** i/lub **Filtrowanie adresów URL**.

Ochrona antywirusowa w usłudze Cyber Protection zapewnia szereg korzyści:

- Znakomitą ochronę na wszystkich etapach działań: proaktywnym, aktywnym i reaktywnym.
- Cztery technologie zabezpieczeń przed złośliwym oprogramowaniem, aby zapewnić najlepszą w swojej klasie wielowarstwową ochronę.
- Zarządzanie oprogramowaniem Microsoft Security Essentials i Microsoft Defender Antivirus.

  Uwaga
  Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Ważne
Plik testu EICAR jest wykrywany tylko pod warunkiem, że w planie ochrony jest włączona opcja **Zaawansowana ochrona przed złośliwym oprogramowaniem**. Jednak niewykrycie pliku EICAR nie wpływa na funkcje ochrony przed złośliwym oprogramowaniem oferowane przez usługę Cyber Protection.

Obsługiwane platformy

Funkcje usługi Active Protection oraz ochrony przed wirusami i złośliwym oprogramowaniem są obsługiwane na następujących platformach.

System operacyjny	Wersja/dystrybucja
Windows	Windows 7 Service Pack 1 lub nowszy Windows Server 2008 R2 Service Pack 1 i nowsze

© Acronis International GmbH, 2003-2024

System operacyjny	Wersja/dystrybucja
	Uwaga W przypadku systemu Windows 7 przed zainstalowaniem agenta ochrony trzeba zainstalować poniższe aktualizacje od firmy Microsoft. • Rozszerzone aktualizacje zabezpieczeń (ESU) systemu Windows 7 • KB4474419 • KB4490628 Więcej informacji na temat wymaganych aktualizacji można znaleźć w tym artykule bazy wiedzy Knowledge Base.
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 i nowsze wersje 6.x, a także 7.x, 8.x Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x lub nowszy

Obsługiwane funkcje na platformach

Uwaga
Ochrona antywirusowa dla systemów Linux i macOS jest dostępna wraz z pakietem Zaawansowana ochrona przed złośliwym oprogramowaniem.

Zestaw funkcji	Windows	Linux	macOS
Ochrona przed wirusami i złośliwym oprogramowaniem			
W pełni zintegrowana funkcja Active Protection	Tak	Nie	Nie
Ochrona antywirusowa w czasie rzeczywistym	Tak	Tak, z pakietem Zaawansowana ochrona przed złośliwym oprogramowaniem	Tak, z pakietem Zaawansowana ochrona przed złośliwym oprogramowaniem
Zaawansowana ochrona przed złośliwym oprogramowaniem w	Tak	Tak	Tak

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Ochrona przed wirusami i złośliwym oprogramowaniem			
czasie rzeczywistym z lokalnym wykrywaniem plików opartym na sygnaturach			
Statyczne analizy przenośnych plików wykonywalnych	Tak	Nie	Tak*
Skanowanie antywirusowe na żądanie	Tak	Tak**	Tak
Ochrona folderów sieciowych	Tak	Tak	Nie
Ochrona po stronie serwera	Tak	Nie	Nie
Skanowanie plików archiwum	Tak	Nie	Tak
Skanowanie dysków wymiennych	Tak	Nie	Tak
Skanowanie tylko nowych i zmienionych plików	Tak	Nie	Tak
Wykluczanie plików/folderów	Tak	Tak	Tak***
Wykluczanie procesów	Tak	Nie	Tak
Mechanizm analiz zachowań	Tak	Nie	Tak
Ochrona przed exploitami	Tak	Nie	Nie
Kwarantanna	Tak	Tak	Tak
Automatyczne czyszczenie kwarantanny	Tak	Tak	Tak
Filtrowanie adresów URL (http/https)	Tak	Nie	Nie
Ogólnofirmowa biała lista	Tak	Nie	Tak
Zarządzanie zaporą****	Tak	Nie	Nie
Zarządzanie programem Microsoft Defender Antivirus*****	Tak	Nie	Nie
Zarządzanie programem Microsoft Security Essentials	Tak	Nie	Nie
Rejestrowanie modułu Ochrona	Tak	Nie	Nie

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Ochrona przed wirusami i złośliwym oprogramowaniem			
przed wirusami i złośliwym oprogramowaniem oraz zarządzanie nim za pośrednictwem Centrum zabezpieczeń systemu Windows			
Dodatkowe informacje na temat obsługiwanych systemów operacyjnych i ich wersji można znaleźć w sekcji "Obsługiwane platformy" (s. 875).			

* Statyczne analizy przenośnych plików wykonywalnych są obsługiwane tylko w przypadku planowanych operacji skanowania w systemie macOS.

** Warunki uruchomienia nie są obsługiwane w przypadku skanowania na żądanie w systemie Linux.

*** Wykluczanie plików/folderów jest obsługiwane tylko w przypadku wskazania plików i folderów, które nie będą skanowane w ramach ochrony w czasie rzeczywistym ani planowanych operacji skanowania w systemie macOS.

**** Zarządzenie zaporą jest dostępne w systemie Windows 8 lub nowszym. System Windows Server nie jest obsługiwany.

***** Zarządzanie programem Microsoft Defender Antivirus jest obsługiwane w systemie Windows 8.1 lub nowszym.

Zestaw funkcji	Windows	Linux	macOS
Active Protection			
Wykrywanie wstrzyknięć procesów	Tak	Nie	Nie
Automatycznie odzyskiwanie plików, których dotyczy problem, z lokalnej pamięci podręcznej	Tak	Tak	Tak
Samoobrona plików kopii zapasowych Acronis	Tak	Nie	Nie
Samoobrona oprogramowania Acronis	Tak	Nie	Tak (Tylko komponenty Active Protection i Ochrona przed złośliwym oprogramowaniem)
Zarządzanie zaufanymi/zablokowanymi procesami	Tak	Nie	Tak

© Acronis International GmbH, 2003-2024

Zestaw funkcji	Windows	Linux	macOS
Active Protection			
Wykluczanie procesów/folderów	Tak	Tak	Tak
Wykrywanie oprogramowania wymuszającego okup na podstawie zachowań procesów (przy użyciu sztucznej inteligencji)	Tak	Tak	Tak
Wykrywanie procesów cryptominingu na podstawie ich zachowań	Tak	Nie	Nie
Ochrona dysków zewnętrznych (HDD, pamięć flash USB, karty SD)	Tak	Nie	Tak
Ochrona folderów sieciowych	Tak	Tak	Tak
Ochrona po stronie serwera	Tak	Nie	Nie
Ochrona programów Zoom, Cisco Webex, Citrix Workspace i Microsoft Teams	Tak	Nie	Nie
Dodatkowe informacje na temat obsługiwanych systemów operacyjnych i ich wersji można znaleźć w sekcji "Obsługiwane platformy" (s. 875).			

Ochrona przed wirusami i złośliwym oprogramowaniem

Uwaga
Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Moduł **Ochrona przed wirusami i złośliwym oprogramowaniem** chroni komputery z systemem Windows, Linux i macOS przed wszystkimi najnowszymi zagrożeniami związanymi ze złośliwym oprogramowaniem. Zobacz pełną listę obsługiwanych funkcji ochrony antywirusowej: "Obsługiwane platformy" (s. 875).

Ochrona przed wirusami i złośliwym oprogramowaniem jest obsługiwana oraz rejestrowana w Centrum zabezpieczeń systemu Windows.

Funkcje antywirusowe

- Wykrywanie złośliwego oprogramowania w plikach w trybie ochrony w czasie rzeczywistym i na żądanie
- Wykrywanie złośliwych zachowań w procesach (w systemie Windows)
- Blokowanie dostępu do złośliwych adresów URL (w systemie Windows)

© Acronis International GmbH, 2003-2024

- Umieszczanie niebezpiecznych plików w kwarantannie
- Dodawanie zaufanych firmowych aplikacji do listy dozwolonych

Typy skanowania

Moduł Ochrona przed wirusami i złośliwym oprogramowaniem można skonfigurować tak, aby działał stale w tle lub był uruchamiany na żądanie.

Ochrona w czasie rzeczywistym

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Funkcja ochrony w czasie rzeczywistym sprawdza wszystkie pliki, które są wykonywane lub otwierane na komputerze, aby zapobiec zagrożeniom związanym ze złośliwym oprogramowaniem.

Aby uniknąć ewentualnych problemów z kompatybilnością i wydajnością, ochrona w czasie rzeczywistym nie może działać równolegle z innymi rozwiązaniami antywirusowymi, które również korzystają z funkcji ochrony w czasie rzeczywistym. Statusy innych zainstalowanych rozwiązań antywirusowych określa się za pośrednictwem Centrum zabezpieczeń systemu Windows. Jeśli komputer z systemem Windows jest już chroniony przez inne rozwiązanie antywirusowe, ochrona w czasie rzeczywistym jest automatycznie wyłączana.

Aby ją włączyć, należy wyłączyć lub odinstalować to inne rozwiązanie antywirusowe. Ochrona w czasie rzeczywistym może automatycznie zastąpić ochronę w czasie rzeczywistym zapewnianą przez usługę Microsoft Defender.

Uwaga
Na komputerach z systemami operacyjnymi Windows Server usługa Microsoft Defender nie będzie wyłączana automatycznie po włączeniu ochrony w czasie rzeczywistym. Administrator musi ręcznie wyłączyć usługę Microsoft Defender, aby uniknąć potencjalnych problemów ze zgodnością.

Można wybrać jeden z poniższych trybów skanowania:

- Wykrywanie w trybie **Inteligentne przy dostępie** oznacza, że program antywirusowy działa w tle i stale aktywnie skanuje system komputera w poszukiwaniu wirusów oraz innych złośliwych zagrożeń, gdy system jest włączony. Złośliwe oprogramowanie zostanie wykryte zarówno podczas wykonywania pliku, jak i podczas różnych operacji dotyczących pliku, np. otwierania go do odczytu lub edycji.
- Wykrywanie w trybie **Skanowanie przy wykonywaniu** oznacza, że skanowane są tylko pliki wykonywalne podczas ich uruchamiania w celu sprawdzenia, czy nie są zainfekowane i nie spowodują żadnych uszkodzeń komputera ani danych. Kopiowanie zainfekowanego pliku nie zostanie wykryte.

© Acronis International GmbH, 2003-2024

Skanowanie planowane

Skanowanie antywirusowe jest przeprowadzane zgodnie z harmonogramem.

Można wybrać jeden z poniższych trybów skanowania.

- **Szybkie skanowanie** — są sprawdzane tylko pliki systemowe obciążenia.
- **Pełne skanowanie** — są sprawdzane wszystkie pliki w obciążeniu.
- **Skanowanie niestandardowe** — są sprawdzane pliki/foldery dodane przez administratora do planu ochrony.

Po zakończeniu skanowania antywirusowego można zobaczyć szczegółowe informacje o obciążeniach, które ucierpiały wskutek danych zagrożeń, w widżecie **Monitorowanie** > **Przegląd** > Ostatnio dotknięte problemem.

Ustawienia modułu Ochrona przed wirusami i złośliwym oprogramowaniem

W tej sekcji opisano funkcje, które można skonfigurować w module **Ochrona przed wirusami i złośliwym oprogramowaniem** w planie ochrony. Instrukcje tworzenia planu ochrony można znaleźć w sekcji "Tworzenie planu ochrony" (s. 222).

W przypadku modułu Ochrona przed wirusami i złośliwym oprogramowaniem można w planie ochrony skonfigurować następujące funkcje:

- "Active Protection" (s. 882)
- "Zaawansowana ochrona przed złośliwym oprogramowaniem" (s. 882)
- "Ochrona folderów sieciowych" (s. 883)
- "Ochrona po stronie serwera" (s. 884)
- "Ochrona własna" (s. 885)
- "Wykrywanie procesów cryptominingu" (s. 886)
- "Kwarantanna" (s. 886)
- "Mechanizm zachowań" (s. 887)
- "Ochrona przed exploitami" (s. 887)
- "Ochrona w czasie rzeczywistym" (s. 889)
- "Zaplanuj skanowanie" (s. 890)
- "Wykluczenia z ochrony" (s. 894)

© Acronis International GmbH, 2003-2024

Uwaga
Nie wszystkie systemy operacyjne obsługują funkcje modułu Ochrona przed wirusami i złośliwym oprogramowaniem. Aby uzyskać więcej informacji na temat obsługiwanych systemów operacyjnych i funkcji, zobacz "Obsługiwane platformy" (s. 875). Niektóre funkcje wymagają określonej licencji, aby były dostępne w planie ochrony.

Active Protection

Usługa Active Protection chroni system przed złośliwym oprogramowaniem znanym jako oprogramowanie wymuszające okup (ransomware), które szyfruje pliki i żąda okupu za klucz szyfrowania.

Ustawienie domyślne: **Włączono**.

Uwaga
Na chronionym komputerze musi być zainstalowany agent ochrony. Dodatkowe informacje na temat obsługiwanych systemów operacyjnych i funkcji można znaleźć w sekcji "Obsługiwane platformy" (s. 875).

Aby skonfigurować usługę Active Protection

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Active Protection**.
3. W sekcji **Działanie po wykryciu** wybierz jedną z dostępnych opcji:

   Ustawienie domyślne: **Cofnij przy użyciu pamięci podręcznej**

   - **Tylko powiadom** — oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania służące wymuszeniu okupu.
   - **Zatrzymaj proces** — oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania służące wymuszeniu okupu i zatrzyma ten proces.
   - **Cofnij przy użyciu pamięci podręcznej** — oprogramowanie wygeneruje alert, zatrzyma proces i wycofa zmiany w pliku przy użyciu pamięci podręcznej usługi.
4. Kliknij **Gotowe**, aby zastosować wybrane opcje do planu ochrony.

Zaawansowana ochrona przed złośliwym oprogramowaniem

Mechanizm ten wykorzystuje rozszerzoną bazę sygnatur wirusów w celu poprawy skuteczności wykrywania złośliwego oprogramowania w ramach zarówno szybkiego, jak i pełnego skanowania.

Ważne
Ta funkcja jest dostępna tylko wtedy, gdy jest włączony pakiet ochrony Zabezpieczenia zaawansowane. Dodatkowe informacje można znaleźć pod adresem https://www.acronis.com/en-us/products/cloud/cyber-protect/security/

© Acronis International GmbH, 2003-2024

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Aby skonfigurować usługę Zaawansowana ochrona przed złośliwym oprogramowaniem

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. W sekcji **Zaawansowana ochrona przed złośliwym oprogramowaniem** użyj przełącznika, aby włączyć lokalny mechanizm oparty na sygnaturach.

Uwaga
Ochrona przed wirusami i złośliwym oprogramowaniem dla systemów macOS i Linux również wymaga lokalnego mechanizmu opartego na sygnaturach. W systemie Windows Ochrona przed wirusami i złośliwym oprogramowaniem jest dostępna bez względu na dostępność takiego mechanizmu.

Ochrona folderów sieciowych

Funkcja **Ochrona folderów sieciowych** pozwala określić, czy moduł Ochrona przed wirusami i złośliwym oprogramowaniem ma chronić foldery sieciowe zamapowane jako dyski lokalne. Ochrona dotyczy folderów udostępnionych przy użyciu protokołów SMB lub NFS.

Aby skonfigurować ochronę folderów sieciowych

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona folderów sieciowych**.
3. Dodaj pliki, w których chcesz utworzyć kopie zapasowe folderów sieciowych:
   - Jeśli na przykład masz obciążenie z systemem Windows, w polu **Windows** wprowadź ścieżkę do pliku systemu Windows, w którym ma zostać utworzona kopia zapasowa folderów sieciowych. Wartość domyślna: C:\ProgramData\Acronis\Restored Network Files.
   - Jeśli na przykład masz obciążenie z systemem macOS, w polu **macOS** wprowadź ścieżkę do plików systemu macOS, w których mają zostać utworzone kopie zapasowe folderów sieciowych. Wartość domyślna: /Library/Application Support/Acronis/Restored Network Files/.

   Uwaga
   Wprowadź ścieżkę do folderu lokalnego. Foldery sieciowe, w tym foldery znajdujące się na zamapowanych dyskach, nie są obsługiwane jako miejsca docelowe kopii zapasowych folderów sieciowych.
4. Kliknij **Gotowe**, aby zastosować wybrane opcje do planu ochrony.

© Acronis International GmbH, 2003-2024

Ochrona po stronie serwera

Funkcja ta pozwala określić, czy usługa Active Protection ma chronić foldery sieciowe udostępnione przez Ciebie przed połączeniami zewnętrznymi przychodzącymi z innych serwerów w sieci, które ewentualnie mogą powodować zagrożenia.

Ustawienie domyślne: **Wyłączone**.

Uwaga
Ochrona po stronie serwera nie jest obsługiwana w systemie Linux.

Aby ustawić zaufane połączenia

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona po stronie serwera**.
3. Użyj przełącznika **Ochrona po stronie serwera**, aby włączyć tę funkcję.
4. Wybierz kartę **Zaufane**.
5. W polu **Zaufane połączenia** kliknij **Dodaj**, aby zdefiniować połączenia, które będą mogły modyfikować dane.
6. W polu **Nazwakomputera/Konto** wpisz nazwę i konto komputera, na którym jest zainstalowany agent ochrony. Na przykład `MyComputer\TestUser`.
7. W polu **Nazwa hosta** wpisz nazwę hosta komputera, który może się łączyć z komputerem przy użyciu agenta ochrony.
8. Aby zapisać definicję połączenia, kliknij znacznik wyboru widoczny po prawej stronie.
9. Kliknij **Gotowe**.

Aby ustawić blokowane połączenia

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona po stronie serwera**.
3. Użyj przełącznika **Ochrona po stronie serwera**, aby włączyć tę funkcję.
4. Wybierz kartę **Zablokowano**.
5. W polu **Zablokowane połączenia** kliknij **Dodaj**, aby zdefiniować połączenia, które nie będą mogły modyfikować danych.
6. W polu **Nazwakomputera/Konto** wpisz nazwę i konto komputera, na którym jest zainstalowany agent ochrony. Na przykład `MyComputer\TestUser`.
7. W polu **Nazwa hosta** wpisz nazwę hosta komputera, który może się łączyć z komputerem przy użyciu agenta ochrony.

© Acronis International GmbH, 2003-2024

8. Aby zapisać definicję połączenia, zaznacz pole wyboru widoczne po prawej stronie.
9. Kliknij **Gotowe**.

Ochrona własna

Ochrona własna zapobiega nieuprawnionym zmianom w procesach własnych oprogramowania, rekordach rejestru, plikach wykonywalnych i konfiguracyjnych oraz kopiach zapasowych przechowywanych w folderach lokalnych.

Administratorzy mogą włączyć opcję **Ochrona własna** bez włączania usługi **Active Protection**.

Ustawienie domyślne: **Włączone**.

Uwaga
Ochrona własna nie jest obsługiwana w systemie Linux.

Aby włączyć funkcję Ochrona własna

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona własna**.
3. Użyj przełącznika **Ochrona własna**, aby włączyć tę funkcję.

Aby włączyć ochronę hasłem

1. Po włączeniu funkcji **Ochrona własna** można włączyć funkcję **Ochrona hasłem** przy użyciu tego przełącznika.
2. Kliknij **Wygeneruj nowe hasło**, aby wygenerować hasło na potrzeby modyfikowania lub usuwania agentów lokalnych.
3. Kliknij **Kopiuj**, a następnie wklej je w bezpiecznym miejscu, ponieważ będzie ono wymagane, jeśli zechcesz lokalnie zmodyfikować listę komponentów.

   Ważne
   Po zamknięciu okna hasło nie będzie dostępne. Aby to hasło zostało zastosowane do urządzeń, należy zapisać ustawienia planu ochrony.

4. Kliknij **Zamknij**.

Ochrona hasłem uniemożliwia nieuprawnionym użytkownikom lub oprogramowaniu odinstalowanie agenta dla systemu Windows lub zmodyfikowanie jego komponentów. Działania te są możliwe dopiero po podaniu hasła, które może udostępnić administrator.

Hasło nie jest nigdy wymagane w przypadku następujących działań:

- Aktualizacja instalacji przez lokalne uruchomienie programu instalacyjnego
- Aktualizacja instalacji przy użyciu konsoli Cyber Protect

© Acronis International GmbH, 2003-2024

- Naprawa instalacji

Ustawienie domyślne: **Wyłączono**

Dodatkowe informacje na temat sposobu włączania funkcji **Ochrona hasłem** można znaleźć w sekcji Zapobieganie nieuprawnionym dezinstalacjom lub modyfikacjom agentów.

Wykrywanie procesów cryptominingu

Złośliwe oprogramowanie do cryptominingu obniża wydajność pożytecznych aplikacji i podwyższa rachunki za energię elektryczną, a generowane przez nie nadmierne obciążenie może powodować awarie systemu, a nawet uszkodzenie sprzętu. Funkcja **Wykrywanie procesów cryptominingu** chroni urządzenia przed złośliwym oprogramowaniem do cryptominingu, zapobiegając nieuprawnionemu korzystaniu z zasobów komputera.

Administratorzy mogą włączyć opcję **Wykrywanie procesów cryptominingu** bez włączania usługi **Active Protection**. Ustawienie domyślne: **Włączono**.

Uwaga
Wykrywanie procesów cryptominingu nie jest obsługiwane w systemie Linux.

Aby skonfigurować ochronę folderów sieciowych

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Wykrywanie procesów cryptominingu**.
3. Użyj przełącznika **Wykrywaj procesy cryptominingu**, aby włączyć lub wyłączyć tę funkcję.
4. Wybierz, co ma zostać zrobione w związku z procesami podejrzewanymi o działania związane z cryptominingiem:
   Ustawienie domyślne: **Zatrzymaj proces**
   - **Tylko powiadom** — oprogramowanie wygeneruje alert.
   - **Zatrzymaj proces** — oprogramowanie wygeneruje alert i zatrzyma proces.
5. Kliknij **Gotowe**, aby zastosować wybrane opcje do planu ochrony.

Kwarantanna

Kwarantanna to folder używany do izolowania podejrzanych (prawdopodobnie zainfekowanych) lub potencjalnie niebezpiecznych plików.

Aby skonfigurować funkcję Kwarantanna

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Kwarantanna**.

© Acronis International GmbH, 2003-2024

3. W polu **Usuń pliki z kwarantanny po** możesz określić liczbę dni, po których upłynięciu pliki poddane kwarantannie zostaną usunięte.
   Ustawienie domyślne: **30 dni**
4. Kliknij **Gotowe**.

Więcej informacji na temat tej funkcji można znaleźć w sekcji Kwarantanna.

Mechanizm zachowań

Funkcja **Mechanizm zachowań** chroni system przed złośliwym oprogramowaniem dzięki zastosowaniu heurystyki behawioralnej do identyfikacji złośliwych procesów.

Ustawienie domyślne: **Włączono**.

Uwaga
Mechanizm zachowań nie jest obsługiwany w systemie Linux.

Aby skonfigurować ochronę folderów sieciowych

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Mechanizm zachowań**.
3. Użyj przełącznika **Mechanizm zachowań**, aby włączyć lub wyłączyć tę funkcję.
4. W sekcji **Działanie po wykryciu** wybierz działanie, które będzie wykonywane przez oprogramowanie po wykryciu aktywności związanej ze złośliwym oprogramowaniem:
   Ustawienie domyślne: **Kwarantanna**
   - **Tylko powiadom** — oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania związane ze złośliwym oprogramowaniem.
   - **Zatrzymaj proces** — oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania związane ze złośliwym oprogramowaniem i zatrzyma ten proces.
   - **Kwarantanna** — oprogramowanie wygeneruje alert, zatrzyma proces i przeniesie pliki wykonywalne do folderu kwarantanny.
5. Kliknij **Gotowe**, aby zastosować wybrane opcje do planu ochrony.

Ochrona przed exploitami

Ważne
Ta funkcja jest dostępna tylko wtedy, gdy jest włączony pakiet ochrony Zabezpieczenia zaawansowane. Dodatkowe informacje można znaleźć pod adresem https://www.acronis.com/en-us/products/cloud/cyber-protect/security/

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

© Acronis International GmbH, 2003-2024

Funkcja ochrony przed exploitami wykrywa i blokuje zainfekowane procesy oraz zapobiega wykorzystywaniu luk w zabezpieczeniach oprogramowania w systemach. W razie wykrycia exploitu oprogramowanie może wygenerować alert dotyczący procesu podejrzewanego o działania związane z exploitami i zatrzymać ten proces.

Ochrona przed exploitami jest dostępna tylko wraz z agentem w wersji 12.5.23130 (21.08, wydany w sierpniu 2020 r.) lub nowszej.

Ustawienie domyślne: **Włączono** w przypadku nowo utworzonych planów ochrony, **Wyłączono** w przypadku istniejących planów ochrony, utworzonych przy użyciu poprzednich wersji agenta.

Uwaga
Ochrona przed exploitami nie jest obsługiwana w systemie Linux.

Możesz wybrać, co ma zrobić program w razie wykrycia exploitu i które metody zapobiegania exploitom ma stosować.

Aby skonfigurować ochronę przed exploitami

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona przed exploitami**.
3. W sekcji **Działanie po wykryciu** wybierz jedną z dostępnych opcji:

   Ustawienie domyślne: **Zatrzymaj proces**

   - **Tylko powiadom**
     Oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania związane z exploitami.
   - **Zatrzymaj proces**
     Oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania związane z exploitami i zatrzyma ten proces.
4. W sekcji **Włączone techniki ochrony przed exploitami** wybierz jedną z dostępnych opcji, aby ją zastosować:
   Ustawienie domyślne: **Wszystkie metody są włączone**

   - **Ochrona pamięci systemowej**
     Wykrywa i blokuje podejrzane modyfikacje praw do wykonywania na stronach pamięci systemowej. Złośliwe procesy stosują takie modyfikacje właściwości stron, aby umożliwić wykonywanie kodów powłoki z poziomu niewykonywalnych obszarów pamięci, np. stosów i stert.
   - **Ochrona przed programowaniem ukierunkowanym na instrukcje powrotu**
     Wykrywa próby wykorzystania techniki exploitów ROP i zapobiega im.
   - **Ochrona przed eskalacją uprawnień**
     Ta funkcja wykrywa i blokuje próby podwyższenia poziomu uprawnień dokonywane przy użyciu nieautoryzowanego kodu lub aplikacji. Eskalacja uprawnień jest wykorzystywana w

© Acronis International GmbH, 2003-2024

ramach złośliwego kodu w celu uzyskania pełnego dostępu do atakowanego komputera, a następnie wykonania krytycznych i wrażliwych zadań. Nieautoryzowany kod nie ma praw dostępu do krytycznych zasobów systemowych ani modyfikacji ustawień systemu.

- **Ochrona przed wstrzyknięciem kodu**

  Ta funkcja wykrywa i blokuje operacje wstrzykiwania złośliwego kodu do procesów zdalnych. Wstrzykiwanie kodu jest stosowanie jako metoda ukrywania złośliwych zadań aplikacji za czystymi lub niezłośliwymi procesami w celu zapobieżenia ich wykryciu przez produkty antywirusowe.

5. Kliknij **Gotowe**, aby zastosować wybrane opcje do planu ochrony.

Uwaga
Procesy umieszczone na liście wykluczeń jako zaufane nie będą skanowane pod kątem exploitów.

Zezwalanie procesom na modyfikowanie kopii zapasowych

Opcja **Zezwól określonym procesom na modyfikowanie kopii zapasowych** jest dostępna tylko wtedy, gdy jest włączone ustawienie **Ochrona własna**.

Dotyczy ona plików o rozszerzeniach .tibx, .tib, .tia, które znajdują się w folderach lokalnych.

To ustawienie pozwala na wskazanie procesów, które mogą modyfikować pliki kopii zapasowych nawet wtedy, gdy pliki te są chronione przez funkcję ochrony własnej. Może to się przydać na przykład w przypadku zamiaru usunięcia plików kopii zapasowej lub przeniesienia ich do innej lokalizacji za pomocą skryptu.

Gdy to ustawienie jest wyłączone, pliki kopii zapasowej mogą być modyfikowane wyłącznie przez proces zatwierdzony przez dostawcę oprogramowania do tworzenia kopii zapasowych. Pozwala to oprogramowaniu na stosowanie reguł przechowywania i usuwanie kopii zapasowych na żądanie użytkownika przesłane za pośrednictwem interfejsu internetowego. Inne procesy – niezależnie od tego, czy zostaną uznane za podejrzane – nie mogą modyfikować kopii zapasowych.

Gdy to ustawienie jest włączone, można zezwolić innym procesom na modyfikowanie kopii zapasowych. Podaj pełną ścieżkę do wykonywalnego procesu, zaczynając od litery dysku.

Ustawienie domyślne: **Wyłączono**.

Ochrona w czasie rzeczywistym

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Funkcja **Ochrona w czasie rzeczywistym** stale sprawdza system komputerowy pod kątem wirusów i innych złośliwych zagrożeń, gdy system jest włączony — chyba że zostanie zatrzymana przez użytkownika komputera.

Ustawienie domyślne: **Włączono**.

© Acronis International GmbH, 2003-2024

Ważne
Ta funkcja jest dostępna tylko wtedy, gdy jest włączony pakiet ochrony Zabezpieczenia zaawansowane. Dodatkowe informacje można znaleźć pod adresem https://www.acronis.com/en-us/products/cloud/cyber-protect/security/

Aby skonfigurować funkcję Ochrona w czasie rzeczywistym

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona w czasie rzeczywistym**.
3. Z listy rozwijanej **Działanie po wykryciu** wybierz jedną z dostępnych opcji:

   Ustawienie domyślne: **Kwarantanna**

   - **Tylko powiadom**

     Oprogramowanie generuje alert dotyczący procesu podejrzewanego o działania służące wymuszeniu okupu.

   - **Zablokuj i powiadom**

     Oprogramowanie blokuje proces i generuje alert dotyczący procesu podejrzewanego o działania związane ze złośliwym oprogramowaniem.

   - **Kwarantanna**
4. Oprogramowanie generuje alert, zatrzymuje proces i przenosi plik wykonywalny do folderu kwarantanny.
5. W sekcji **Tryb skanowania** wybierz działanie wykonywane przez oprogramowanie po wykryciu wirusa lub innego złośliwego zagrożenia:

   Ustawienie domyślne: **Inteligentne przy dostępie**

   - **Inteligentne przy dostępie** — monitorowane są wszystkie działania w systemie i automatycznie są skanowane pliki, gdy są one otwierane w celu odczytania lub zapisania oraz gdy jest uruchamiany program.
   - **Przy wykonywaniu** — automatycznie są skanowane tylko pliki wykonywalne w chwili ich uruchamiania w celu sprawdzenia, czy nie są zainfekowane i nie spowodują żadnych uszkodzeń komputera lub danych.
6. Kliknij **Gotowe**.

Zaplanuj skanowanie

Skanowanie na żądanie sprawdza system komputerowy w poszukiwaniu wirusów według określonego harmonogramu. Podczas pełnego skanowania sprawdzane są wszystkie pliki na komputerze, a podczas szybkiego skanowania — tylko pliki systemowe.

Aby skonfigurować funkcję Zaplanuj skanowanie

Ustawienia domyślne:

© Acronis International GmbH, 2003-2024

- opcja **Skanowanie niestandardowe** jest wyłączona.
- Zaplanowano skanowanie **Szybkie** i **Pełne**.

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Zaplanuj skanowanie**.
3. Użyj tego przełącznika, aby włączyć typ skanowania, które chcesz zastosować w przypadku swojego urządzenia.

Dostępne typy skanowania:

- **Pełne** — trwa znacznie dłużej niż szybkie skanowanie, ponieważ w tym przypadku jest sprawdzany każdy plik.
- **Szybkie** — w ramach szybkiego skanowania sprawdzane są tylko typowe obszary na komputerze, w których zwykle znajduje się złośliwe oprogramowanie.
- **Niestandardowe** — sprawdzane są pliki/foldery wybrane przez administratora planu usługi Ochrona.

Uwaga
Wszystkie trzy tryby skanowania — **Szybkie**, **Pełne** i **Niestandardowe** — można zaplanować w jednym planie ochrony.

Aby skonfigurować skanowanie niestandardowe

- Użyj **przełącznika Skanowanie niestandardowe**, aby włączyć lub wyłączyć skanowanie tego typu.
- Z listy rozwijanej **Działanie po wykryciu** wybierz jedną z dostępnych opcji:

Ustawienie domyślne: **Kwarantanna**

Kwarantanna

Oprogramowanie generuje alert i przenosi plik wykonywalny do folderu kwarantanny.

Tylko powiadom

Oprogramowanie generuje alert dotyczący procesu podejrzewanego o działania związane ze złośliwym oprogramowaniem.

Pole	Opis
Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń	To ustawienie umożliwia określenie czasu uruchomienia zadania. Dostępne są następujące wartości: • **Zaplanuj według czasu** — jest to ustawienie domyślne. Zadanie zostanie uruchomione w określonym czasie. • **Gdy użytkownik zaloguje się w systemie** — domyślnie zalogowanie się dowolnego użytkownika spowoduje wyzwolenie

© Acronis International GmbH, 2003-2024

Pole	Opis
	zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika. • **Gdy użytkownik wyloguje się z systemu** — domyślnie wylogowanie się dowolnego użytkownika spowoduje wyzwolenie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika. **Uwaga** Zadanie nie zostanie uruchomione przy zamykaniu systemu. Zamknięcie systemu i wylogowanie to różne zdarzenia w konfiguracji harmonogramu. • **Podczas uruchamiania systemu** — zadanie zostanie uruchomione podczas uruchamiania systemu operacyjnego. • **Podczas zamknięcia systemu** — zadanie zostanie uruchomione podczas zamykania systemu operacyjnego.
Typ harmonogramu	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Dostępne są następujące wartości: • **Co miesiąc** — należy wybrać miesiące i tygodnie lub dni miesiąca, w których zadanie będzie uruchamiane. • **Codziennie** — jest to ustawienie domyślne. Wybierz dni tygodnia, w które będzie uruchamiane zadanie. • **Co godzinę** — należy wybrać dni tygodnia, liczbę powtórzeń oraz przedział czasu, w których zadanie będzie uruchamiane.
Czas rozpoczęcia	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu** Wybierz dokładną godzinę, o której zostanie uruchomione zadanie.
Uruchom w podanym okresie	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Ustaw zakres czasu, w którym będzie obowiązywać skonfigurowany harmonogram.
Określ konto użytkownika, którego zalogowanie się w systemie operacyjnym	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Gdy użytkownik zaloguje się w systemie**. Dostępne są następujące wartości: • **Dowolny użytkownik** — użyj tej opcji, jeśli chcesz, aby zalogowanie

© Acronis International GmbH, 2003-2024

Pole	Opis
zainicjuje wykonanie zadania	się dowolnego użytkownika powodowało wyzwolenie zadania. • **Następujący użytkownik** — użyj tej opcji, jeśli chcesz, aby tylko zalogowanie się na określonym koncie użytkownika powodowało wyzwolenie zadania.
Określ konto użytkownika, którego wylogowanie się z systemu operacyjnego zainicjuje wykonanie zadania	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Gdy użytkownik wyloguje się z systemu**. Dostępne są następujące wartości: • **Dowolny użytkownik** — użyj tej opcji, jeśli chcesz, aby wylogowanie się dowolnego użytkownika powodowało wyzwolenie zadania. • **Następujący użytkownik** — użyj tej opcji, jeśli chcesz, aby tylko wylogowanie się z określonego konta użytkownika powodowało wyzwolenie zadania.
Warunki rozpoczęcia	Określ wszystkie warunki, które muszą być jednocześnie spełnione, aby zostało uruchomione zadanie. Warunki rozpoczęcia skanowania pod kątem złośliwego oprogramowania są podobne do warunków uruchomienia modułu **Kopia zapasowa**, które opisano w sekcji „Warunki rozpoczęcia”. Można zdefiniować następujące dodatkowe warunki uruchomienia: • **Rozłóż rozpoczęcie zadania w przedziale czasu** — ta opcja umożliwia zdefiniowanie ram czasowych zadań, aby uniknąć wąskich gardeł na łączach sieciowych. Możesz określić opóźnienie w godzinach lub minutach. Jeśli na przykład domyślną godziną rozpoczęcia jest 10:00, a opóźnienie wynosi 60 minut, to zadanie rozpocznie się między godziną 10:00 a 11:00. • **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu** • **Zablokuj włączanie trybu uśpienia lub hibernacji podczas wykonywania zadania** — ta opcja działa tylko w przypadku komputerów z systemem Windows. • **Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie po** — określ czas, po którym zadanie zostanie uruchomione, bez względu na spełnienie innych warunków rozpoczęcia. **Uwaga** Warunki uruchomienia nie są obsługiwane w systemie Linux.

- Zaznacz pole wyboru **Skanuj tylko nowe i zmienione pliki**, jeśli mają zostać przeskanowane tylko nowo utworzone i zmodyfikowane pliki.

© Acronis International GmbH, 2003-2024

Ustawienie domyślne: **Włączono**

- Dwie dodatkowe opcje wyświetlane tylko w przypadku ustawień **Skanowanie niestandardowe** lub **Skanowanie pełne**:

1. **Skanuj pliki archiwum**

   Ustawienie domyślne: **Włączono**.

   Maksymalna głębokość rekursji

   Ustawienie domyślne: **16**

   Liczba poziomów osadzonych archiwów, które można przeskanować. Na przykład dokument MIME > archiwum ZIP > archiwum pakietu Office > zawartość dokumentu.

   Maksymalny rozmiar

   Ustawienie domyślne: **100**

   Maksymalny rozmiar pliku archiwum do przeskanowania.

2. **Skanuj dyski wymienne**

Ustawienie domyślne: **Wyłączono**

- **Zamapowane (zdalne) dyski sieciowe**
- **Urządzenia pamięci USB** (takie jak pamięć flash i zewnętrzne dyski twarde)
- **Dyski CD/DVD**

Uwaga
Skanowanie dysków wymiennych nie jest obsługiwane w systemie Linux.

Wykluczenia z ochrony

Wykluczenia z ochrony pozwalają wyeliminować fałszywe zgłoszenia w sytuacji, gdy zaufany program zostanie uznany za ransomware lub złośliwe oprogramowanie. Zaufane i zablokowane elementy można zdefiniować przez dodanie ich do listy wykluczeń z ochrony.

Do listy zaufanych elementów można dodawać pliki, procesy i foldery. Sprawi to, że będą one uznawane za bezpieczne w systemie i zapobiegnie wykrywaniu ich w przyszłości.

Do listy zablokowanych elementów można dodawać procesy i skróty. Gwarantuje to blokowanie takich procesów i ochronę bezpieczeństwa obciążenia.

Element do wykluczenia z ochrony	Zablokowano	Zaufane
Skrót	W przypadku dodania skrótu do listy zablokowanych system zatrzyma proces na podstawie podanego	W przypadku dodania skrótu do listy zaufanych system na podstawie podanego skrótu będzie wiedzieć,

© Acronis International GmbH, 2003-2024

Element do wykluczenia z ochrony	Zablokowano	Zaufane
	skrótu. Na przykład w przypadku dodania skrótu MD5 938c2cc0dcc05f2b68c4287040cfcf71 będzie blokowany proces związany z tym skrótem.	który proces ma być ignorowany przez funkcję monitorowania. Na przykład w przypadku dodania skrótu MD5 938c2cc0dcc05f2b68c4287040cfcf71 związany z nim proces zostanie uznany za zaufany i wykluczony z monitorowania.
Proces	W przypadku dodania procesu do listy zablokowanych system będzie wiedzieć, że dany proces musi być monitorowany — i zawsze blokowany. Na przykład w przypadku dodania ścieżki C:\Users\user1\application\nppInstaller.exe do listy zablokowanych proces ten będzie blokowany i nie uda Ci się go uruchomić, jeśli podejmiesz taką próbę.	W przypadku dodania procesu do listy zaufanych system będzie wiedzieć, że dany proces ma zostać wykluczony z monitorowania. **Uwaga** Procesy podpisane przez firmę Microsoft są zawsze zaufane. Na przykład w przypadku dodania ścieżki C:\Users\user1\application\nppInstaller.exe proces ten zostanie wykluczony z monitorowania i program antywirusowy nie będzie zakłócał działania tego procesu.
Plik/folder		W przypadku dodania pliku lub folderu do listy zaufanych system będzie wiedzieć, że dany plik lub folder zawsze ma być uznawany za bezpieczny i nie trzeba go skanować/monitorować.

Aby wskazać elementy, które zawsze będą traktowane jako zaufane

1. Otwórz plan ochrony.
2. Rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
3. Zaznacz opcję **Wykluczenia**.
   Zostanie otwarte okno **Wykluczenia z ochrony**.
4. W sekcji **Elementy zaufane** kliknij **Dodaj**, aby wybrać jedną z dostępnych opcji:
   - Aby skonfigurować jako zaufany plik, folder lub proces, zaznacz opcję **Plik/folder/proces**.
     Zostanie otwarte okno **Dodaj plik/folder/proces**.

© Acronis International GmbH, 2003-2024

- W polu **Plik/proces/folder** wprowadź w osobnych wierszach ścieżki do każdego procesu, folderu lub pliku. W sekcji **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów zaufanych.
- Zaznacz pole wyboru **Dodaj jako plik/folder**, aby skonfigurować plik/folder jako zaufany. Przykłady opisów folderów: D:\folder\, /home/Folder/folder2, F:\
- Zaznacz pole wyboru **Dodaj jako proces**, aby skonfigurować proces jako zaufany. Wybrane procesy zostaną wykluczone z monitorowania.

Uwaga
Podaj pełną ścieżkę do wykonywalnego procesu, zaczynając od litery dysku. Na przykład `C:\Windows\Temp\er76s7sdkh.exe`.

Uwaga
Obsługiwane są lokalne ścieżki sieciowe, na przykład: \\localhost\ścieżkafolderu\plik.exe.

- Zaznacz opcję **Skrót**, aby dodać skróty MD5 do listy zaufanych elementów. Zostanie otwarte okno **Dodaj skrót**.
  - W tym miejscu możesz wstawić w osobnych wierszach skróty MD5, które mają zostać dodane jako zaufane do listy wykluczeń z ochrony. Na podstawie tej listy program Cyber Protection wykluczy z monitorowania procesy wskazane za pomocą skrótów MD5.

Ustawienie domyślne: Domyślnie nie ma zdefiniowanych żadnych wyjątków.

Aby określić elementy, które zawsze będą blokowane

1. Otwórz plan ochrony.
2. Rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
3. Zaznacz opcję **Wykluczenia z ochrony**. Zostanie otwarte okno **Wykluczenia z ochrony**.

W sekcji **Elementy blokowane** kliknij **Dodaj**, aby wybrać jedną z dostępnych opcji:

- Aby były blokowane procesy, zaznacz opcję **Proces**. Zostanie otwarte okno **Dodaj proces**.
  - W polu **Proces** wprowadź w osobnych wierszach ścieżki do poszczególnych procesów. W polu **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów blokowanych.

Uwaga
Dopóki na komputerze jest włączona funkcja Active Protection, procesy te nie będą mogły się rozpocząć.

- Aby były blokowane skróty, zaznacz opcję **Skrót**. Zostanie wyświetlone okno **Dodaj skrót**.
  - W polu **Skrót** wprowadź w osobnych wierszach skróty poszczególnych procesów. W polu **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów blokowanych.

Ustawienie domyślne: Domyślnie nie ma zdefiniowanych żadnych wyjątków.

© Acronis International GmbH, 2003-2024

Symbole wieloznaczne

W celu wskazania folderów można używać symboli wieloznacznych * i ?. Gwiazdka (*) zastępuje zero lub więcej znaków. Znak zapytania (?) zastępuje dokładnie jeden znak. Zmiennych środowiskowych, takich jak `%AppData%` nie można używać.

Dodając elementy do list wykluczeń, można używać symbolu wieloznacznego (*).

- Symbole wieloznaczne można stosować w środku lub na końcu opisu.

Przykłady dopuszczalnego użycia symboli wieloznacznych w opisach:

C:*.pdf

D:\folders\plik.*

C:\Użytkownicy*\AppData\Roaming

- Symboli wieloznacznych nie można stosować na początku opisu.

Przykłady niedopuszczalnego użycia symboli wieloznacznych w opisach:

*.docx

*:\folder\

Zmienne

W celu dodania elementów do listy wykluczeń z ochrony można też używać zmiennych, jednak występują następujące ograniczenia:

- W przypadku systemu Windows obsługiwane są tylko zmienne SYSTEMOWE. Zmienne dotyczące użytkowników, takie jak %USERNAME% czy %APPDATA%, nie są obsługiwane. Zmienne z wartością {username} nie są obsługiwane. Więcej informacji można znaleźć pod adresem https://ss64.com/nt/syntax-variables.html.
- W przypadku systemu macOS zmienne środowiskowe nie są obsługiwane.
- W przypadku systemu Linux zmienne środowiskowe nie są obsługiwane.

Przykłady obsługiwanych formatów:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Opis

W polu **Opis** można wpisać uwagi na temat wykluczeń dodanych do listy wykluczeń z ochrony. Oto garść podpowiedzi dotyczących ewentualnych uwag:

© Acronis International GmbH, 2003-2024

- Przyczyny i cele wykluczenia.
- Rzeczywista nazwa pliku wykluczonego przy użyciu skrótu.
- Sygnatury czasowe.

Jeśli w jednym wpisie dodano więcej niż jeden element, można zarejestrować tylko 1 komentarz dotyczący wszystkich tych elementów.

Active Protection w wersji Cyber Backup Standard

W wersji Cyber Backup Standard Edition Active Protection jest osobnym modułem w planie ochrony. Moduł ten można osobno konfigurować i stosować do innych urządzeń lub grup urządzeń.

W przypadku wszystkich innych wersji usługi Cyber Protection funkcja Active Protection jest częścią modułu **Ochrona przed wirusami i złośliwym oprogramowaniem** planu ochrony.

Ustawienie domyślne: **Włączono**.

Uwaga
Na chronionym komputerze musi być zainstalowany agent ochrony. Dodatkowe informacje na temat obsługiwanych systemów operacyjnych i funkcji można znaleźć w sekcji "Obsługiwane platformy" (s. 875).

Sposób działania

Funkcja Active Protection monitoruje procesy działające na chronionym komputerze. Gdy jakiś zewnętrzny proces próbuje zaszyfrować pliki lub dokonać cryptominingu, moduł Active Protection generuje alert i podejmuje dodatkowe działania określone w planie ochrony.

Ponadto funkcja Active Protection zapobiega nieuprawnionym zmianom we własnych procesach oprogramowania do tworzenia kopii zapasowych, rekordach rejestru, plikach wykonywalnych i konfiguracyjnych oraz kopiach zapasowych przechowywanych w folderach lokalnych.

Do identyfikacji złośliwych procesów funkcja Active Protection używa heurystyki behawioralnej. Funkcja Active Protection porównuje łańcuch działań wykonanych przez proces z łańcuchami zdarzeń zapisanych w bazie danych wzorców złośliwego zachowania. Takie podejście umożliwia funkcji Active Protection wykrycie nowego złośliwego oprogramowania na podstawie jego typowego zachowania.

Ustawienia usługi Active Protection w oprogramowaniu Cyber Backup Standard

W wersji Cyber Backup Standard można skonfigurować następujące funkcje modułu Active Protection:

- Działanie po wykryciu
- Ochrona własna

© Acronis International GmbH, 2003-2024

- Ochrona folderów sieciowych
- Ochrona po stronie serwera
- Wykrywanie procesów cryptominingu
- Wykluczenia

Uwaga
Moduł Active Protection dla systemu Linux obsługuje następujące ustawienia: Działanie po wykryciu, Ochrona folderów sieciowych i Wykluczenia. Ochrona folderów sieciowych jest zawsze włączona i nie można jej konfigurować.

Działanie po wykryciu

W sekcji **Działanie po wykryciu** wybierz jedną z dostępnych opcji:

- **Tylko powiadom**
  Oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania służące wymuszeniu okupu.
- **Zatrzymaj proces**
  Oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania służące wymuszeniu okupu i zatrzyma ten proces.
- **Cofnij przy użyciu pamięci podręcznej**
  Oprogramowanie wygeneruje alert, zatrzyma proces i wycofa zmiany w pliku przy użyciu pamięci podręcznej usługi.

Ustawienie domyślne: **Cofnij przy użyciu pamięci podręcznej**.

Ochrona własna zapobiega nieuprawnionym zmianom w procesach własnych oprogramowania, rekordach rejestru, plikach wykonywalnych i konfiguracyjnych oraz kopiach zapasowych przechowywanych w folderach lokalnych.

Administratorzy mogą włączyć opcję **Ochrona własna** bez włączania usługi **Active Protection**.

Ustawienie domyślne: **Włączone**.

Uwaga
Ochrona własna nie jest obsługiwana w systemie Linux.

Aby włączyć funkcję Ochrona własna

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona własna**.
3. Użyj przełącznika **Ochrona własna**, aby włączyć tę funkcję.

Aby włączyć ochronę hasłem

© Acronis International GmbH, 2003-2024

1. Po włączeniu funkcji **Ochrona własna** można włączyć funkcję **Ochrona hasłem** przy użyciu tego przełącznika.
2. Kliknij **Wygeneruj nowe hasło**, aby wygenerować hasło na potrzeby modyfikowania lub usuwania agentów lokalnych.
3. Kliknij **Kopiuj**, a następnie wklej je w bezpiecznym miejscu, ponieważ będzie ono wymagane, jeśli zechcesz lokalnie zmodyfikować listę komponentów.

   Ważne
   Po zamknięciu okna hasło nie będzie dostępne. Aby to hasło zostało zastosowane do urządzeń, należy zapisać ustawienia planu ochrony.

4. Kliknij **Zamknij**.

Ochrona hasłem uniemożliwia nieuprawnionym użytkownikom lub oprogramowaniu odinstalowanie agenta dla systemu Windows lub zmodyfikowanie jego komponentów. Działania te są możliwe dopiero po podaniu hasła, które może udostępnić administrator.

Hasło nie jest nigdy wymagane w przypadku następujących działań:

- Aktualizacja instalacji przez lokalne uruchomienie programu instalacyjnego
- Aktualizacja instalacji przy użyciu konsoli Cyber Protect
- Naprawa instalacji

Ustawienie domyślne: **Wyłączono**

Dodatkowe informacje na temat sposobu włączania funkcji **Ochrona hasłem** można znaleźć w sekcji Zapobieganie nieuprawnionym dezinstalacjom lub modyfikacjom agentów.

Ochrona folderów sieciowych

Ustawienie **Chroń foldery sieciowe zamapowane jako dyski lokalne** pozwala określić, czy usługa Active Protection ma chronić foldery sieciowe zamapowane jako dyski lokalne przed lokalnymi złośliwymi procesami.

Ustawienie to dotyczy folderów udostępnianych za pomocą protokołów SMB lub NFS.

Jeśli plik pierwotnie znajdował się na zamapowanym dysku, nie można go zapisać w pierwotnej lokalizacji po wyodrębnieniu z pamięci podręcznej za pomocą opcji **Cofnij przy użyciu pamięci podręcznej**. Zamiast tego plik zostanie zapisany w folderze określonym w tym ustawieniu. Domyślny folder to `C:\ProgramData\Acronis\Restored Network Files` w przypadku systemu Windows i `Library/Application Support/Acronis/Restored Network Files/` w przypadku systemu macOS. Jeśli taki folder nie istnieje, zostanie utworzony. Jeśli chcesz zmienić tę ścieżkę, wskaż folder lokalny. Foldery sieciowe, w tym foldery znajdujące się na zamapowanych dyskach, nie są obsługiwane.

Ustawienie domyślne: **Włączone**.

© Acronis International GmbH, 2003-2024

Funkcja ta pozwala określić, czy usługa Active Protection ma chronić foldery sieciowe udostępnione przez Ciebie przed połączeniami zewnętrznymi przychodzącymi z innych serwerów w sieci, które ewentualnie mogą powodować zagrożenia.

Ustawienie domyślne: **Wyłączone**.

Uwaga
Ochrona po stronie serwera nie jest obsługiwana w systemie Linux.

Aby ustawić zaufane połączenia

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona po stronie serwera**.
3. Użyj przełącznika **Ochrona po stronie serwera**, aby włączyć tę funkcję.
4. Wybierz kartę **Zaufane**.
5. W polu **Zaufane połączenia** kliknij **Dodaj**, aby zdefiniować połączenia, które będą mogły modyfikować dane.
6. W polu **Nazwakomputera/Konto** wpisz nazwę i konto komputera, na którym jest zainstalowany agent ochrony. Na przykład `MyComputer\TestUser`.
7. W polu **Nazwa hosta** wpisz nazwę hosta komputera, który może się łączyć z komputerem przy użyciu agenta ochrony.
8. Aby zapisać definicję połączenia, kliknij znacznik wyboru widoczny po prawej stronie.
9. Kliknij **Gotowe**.

Aby ustawić blokowane połączenia

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Ochrona po stronie serwera**.
3. Użyj przełącznika **Ochrona po stronie serwera**, aby włączyć tę funkcję.
4. Wybierz kartę **Zablokowano**.
5. W polu **Zablokowane połączenia** kliknij **Dodaj**, aby zdefiniować połączenia, które nie będą mogły modyfikować danych.
6. W polu **Nazwakomputera/Konto** wpisz nazwę i konto komputera, na którym jest zainstalowany agent ochrony. Na przykład `MyComputer\TestUser`.
7. W polu **Nazwa hosta** wpisz nazwę hosta komputera, który może się łączyć z komputerem przy użyciu agenta ochrony.
8. Aby zapisać definicję połączenia, zaznacz pole wyboru widoczne po prawej stronie.
9. Kliknij **Gotowe**.

© Acronis International GmbH, 2003-2024

Złośliwe oprogramowanie do cryptominingu obniża wydajność pożytecznych aplikacji i podwyższa rachunki za energię elektryczną, a generowane przez nie nadmierne obciążenie może powodować awarie systemu, a nawet uszkodzenie sprzętu. Funkcja **Wykrywanie procesów cryptominingu** chroni urządzenia przed złośliwym oprogramowaniem do cryptominingu, zapobiegając nieuprawnionemu korzystaniu z zasobów komputera.

Administratorzy mogą włączyć opcję **Wykrywanie procesów cryptominingu** bez włączania usługi **Active Protection**. Ustawienie domyślne: **Włączono**.

Uwaga
Wykrywanie procesów cryptominingu nie jest obsługiwane w systemie Linux.

Aby skonfigurować ochronę folderów sieciowych

1. W oknie **Utwórz plan ochrony** rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
2. Kliknij **Wykrywanie procesów cryptominingu**.
3. Użyj przełącznika **Wykrywaj procesy cryptominingu**, aby włączyć lub wyłączyć tę funkcję.
4. Wybierz, co ma zostać zrobione w związku z procesami podejrzewanymi o działania związane z cryptominingiem:
   Ustawienie domyślne: **Zatrzymaj proces**
   - **Tylko powiadom** — oprogramowanie wygeneruje alert.
   - **Zatrzymaj proces** — oprogramowanie wygeneruje alert i zatrzyma proces.
5. Kliknij **Gotowe**, aby zastosować wybrane opcje do planu ochrony.

Wykluczenia z ochrony pozwalają wyeliminować fałszywe zgłoszenia w sytuacji, gdy zaufany program zostanie uznany za ransomware lub złośliwe oprogramowanie. Zaufane i zablokowane elementy można zdefiniować przez dodanie ich do listy wykluczeń z ochrony.

Do listy zaufanych elementów można dodawać pliki, procesy i foldery. Sprawi to, że będą one uznawane za bezpieczne w systemie i zapobiegnie wykrywaniu ich w przyszłości.

Do listy zablokowanych elementów można dodawać procesy i skróty. Gwarantuje to blokowanie takich procesów i ochronę bezpieczeństwa obciążenia.

Element do wykluczenia z ochrony	Zablokowano	Zaufane
Skrót	W przypadku dodania skrótu do listy zablokowanych system zatrzyma proces na podstawie podanego skrótu.	W przypadku dodania skrótu do listy zaufanych system na podstawie podanego skrótu będzie wiedzieć, który proces ma być ignorowany przez funkcję monitorowania.

© Acronis International GmbH, 2003-2024

Element do wykluczenia z ochrony	Zablokowano	Zaufane
	Na przykład w przypadku dodania skrótu MD5 938c2cc0dcc05f2b68c4287040cfcf71 będzie blokowany proces związany z tym skrótem.	Na przykład w przypadku dodania skrótu MD5 938c2cc0dcc05f2b68c4287040cfcf71 związany z nim proces zostanie uznany za zaufany i wykluczony z monitorowania.
Proces	W przypadku dodania procesu do listy zablokowanych system będzie wiedzieć, że dany proces musi być monitorowany — i zawsze blokowany. Na przykład w przypadku dodania ścieżki C:\Users\user1\application\nppInstaller.exe do listy zablokowanych proces ten będzie blokowany i nie uda Ci się go uruchomić, jeśli podejmiesz taką próbę.	W przypadku dodania procesu do listy zaufanych system będzie wiedzieć, że dany proces ma zostać wykluczony z monitorowania. **Uwaga** Procesy podpisane przez firmę Microsoft są zawsze zaufane. Na przykład w przypadku dodania ścieżki C:\Users\user1\application\nppInstaller.exe proces ten zostanie wykluczony z monitorowania i program antywirusowy nie będzie zakłócał działania tego procesu.
Plik/folder		W przypadku dodania pliku lub folderu do listy zaufanych system będzie wiedzieć, że dany plik lub folder zawsze ma być uznawany za bezpieczny i nie trzeba go skanować/monitorować.

Aby wskazać elementy, które zawsze będą traktowane jako zaufane

1. Otwórz plan ochrony.
2. Rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
3. Zaznacz opcję **Wykluczenia**.
   Zostanie otwarte okno **Wykluczenia z ochrony**.
4. W sekcji **Elementy zaufane** kliknij **Dodaj**, aby wybrać jedną z dostępnych opcji:
   - Aby skonfigurować jako zaufany plik, folder lub proces, zaznacz opcję **Plik/folder/proces**.
     Zostanie otwarte okno **Dodaj plik/folder/proces**.
     - W polu **Plik/proces/folder** wprowadź w osobnych wierszach ścieżki do każdego procesu, folderu lub pliku. W sekcji **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów zaufanych.

© Acronis International GmbH, 2003-2024

- Zaznacz pole wyboru **Dodaj jako plik/folder**, aby skonfigurować plik/folder jako zaufany. Przykłady opisów folderów: D:\folder\, /home/Folder/folder2, F:\
- Zaznacz pole wyboru **Dodaj jako proces**, aby skonfigurować proces jako zaufany. Wybrane procesy zostaną wykluczone z monitorowania.

  Uwaga
  Podaj pełną ścieżkę do wykonywalnego procesu, zaczynając od litery dysku. Na przykład `C:\Windows\Temp\er76s7sdkh.exe`.

  Uwaga
  Obsługiwane są lokalne ścieżki sieciowe, na przykład: \\localhost\ścieżkafolderu\plik.exe.

- Zaznacz opcję **Skrót**, aby dodać skróty MD5 do listy zaufanych elementów. Zostanie otwarte okno **Dodaj skrót**.
  - W tym miejscu możesz wstawić w osobnych wierszach skróty MD5, które mają zostać dodane jako zaufane do listy wykluczeń z ochrony. Na podstawie tej listy program Cyber Protection wykluczy z monitorowania procesy wskazane za pomocą skrótów MD5.

Ustawienie domyślne: Domyślnie nie ma zdefiniowanych żadnych wyjątków.

Aby określić elementy, które zawsze będą blokowane

1. Otwórz plan ochrony.
2. Rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**.
3. Zaznacz opcję **Wykluczenia z ochrony**. Zostanie otwarte okno **Wykluczenia z ochrony**.

   W sekcji **Elementy blokowane** kliknij **Dodaj**, aby wybrać jedną z dostępnych opcji:
- Aby były blokowane procesy, zaznacz opcję **Proces**. Zostanie otwarte okno **Dodaj proces**.
  - W polu **Proces** wprowadź w osobnych wierszach ścieżki do poszczególnych procesów. W polu **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów blokowanych.

  Uwaga
  Dopóki na komputerze jest włączona funkcja Active Protection, procesy te nie będą mogły się rozpocząć.

- Aby były blokowane skróty, zaznacz opcję **Skrót**. Zostanie wyświetlone okno **Dodaj skrót**.
  - W polu **Skrót** wprowadź w osobnych wierszach skróty poszczególnych procesów. W polu **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów blokowanych.

Ustawienie domyślne: Domyślnie nie ma zdefiniowanych żadnych wyjątków.

Symbole wieloznaczne

W celu wskazania folderów można używać symboli wieloznacznych * i ?. Gwiazdka (*) zastępuje zero lub więcej znaków. Znak zapytania (?) zastępuje dokładnie jeden znak. Zmiennych środowiskowych,

© Acronis International GmbH, 2003-2024

takich jak `%AppData%` nie można używać.

Dodając elementy do list wykluczeń, można używać symbolu wieloznacznego (*).

- Symbole wieloznaczne można stosować w środku lub na końcu opisu.

Przykłady dopuszczalnego użycia symboli wieloznacznych w opisach:

C:*.pdf

D:\folders\plik.*

C:\Użytkownicy*\AppData\Roaming

- Symboli wieloznacznych nie można stosować na początku opisu.

Przykłady niedopuszczalnego użycia symboli wieloznacznych w opisach:

*.docx

*:\folder\

Zmienne

W celu dodania elementów do listy wykluczeń z ochrony można też używać zmiennych, jednak występują następujące ograniczenia:

- W przypadku systemu Windows obsługiwane są tylko zmienne SYSTEMOWE. Zmienne dotyczące użytkowników, takie jak %USERNAME% czy %APPDATA%, nie są obsługiwane. Zmienne z wartością {username} nie są obsługiwane. Więcej informacji można znaleźć pod adresem https://ss64.com/nt/syntax-variables.html.
- W przypadku systemu macOS zmienne środowiskowe nie są obsługiwane.
- W przypadku systemu Linux zmienne środowiskowe nie są obsługiwane.

Przykłady obsługiwanych formatów:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

Opis

W polu **Opis** można wpisać uwagi na temat wykluczeń dodanych do listy wykluczeń z ochrony. Oto garść podpowiedzi dotyczących ewentualnych uwag:

- Przyczyny i cele wykluczenia.
- Rzeczywista nazwa pliku wykluczonego przy użyciu skrótu.
- Sygnatury czasowe.

© Acronis International GmbH, 2003-2024

Jeśli w jednym wpisie dodano więcej niż jeden element, można zarejestrować tylko 1 komentarz dotyczący wszystkich tych elementów.

Filtrowanie adresów URL

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Złośliwe oprogramowanie jest często rozprowadzane przez złośliwe lub zainfekowane witryny internetowe i wykorzystuje metodę infekcji Drive-by download, czyli niepożądane pobieranie plików.

Funkcja Filtrowanie adresów URL umożliwia chronienie komputerów przed takimi zagrożeniami pochodzącymi z Internetu jak złośliwe oprogramowanie czy phishing. Organizację można chronić przez blokowanie dostępu użytkowników do witryn internetowych, które mogą mieć złośliwą zawartość.

Filtrowanie adresów URL pozwala również na kontrolowanie użytkowania stron internetowych w celu zapewnienia zgodności z zewnętrznymi przepisami i wewnętrznymi zasadami firmy. Dostęp do witryn internetowych można konfigurować na podstawie kategorii, której dotyczą. Obecnie funkcja Filtrowanie adresów URL obsługuje 44 kategorie witryn internetowych i zarządzanie dostępem do nich.

Teraz połączenia HTTP/HTTPS na komputerach z systemem Windows będą sprawdzane przez agenta ochrony.

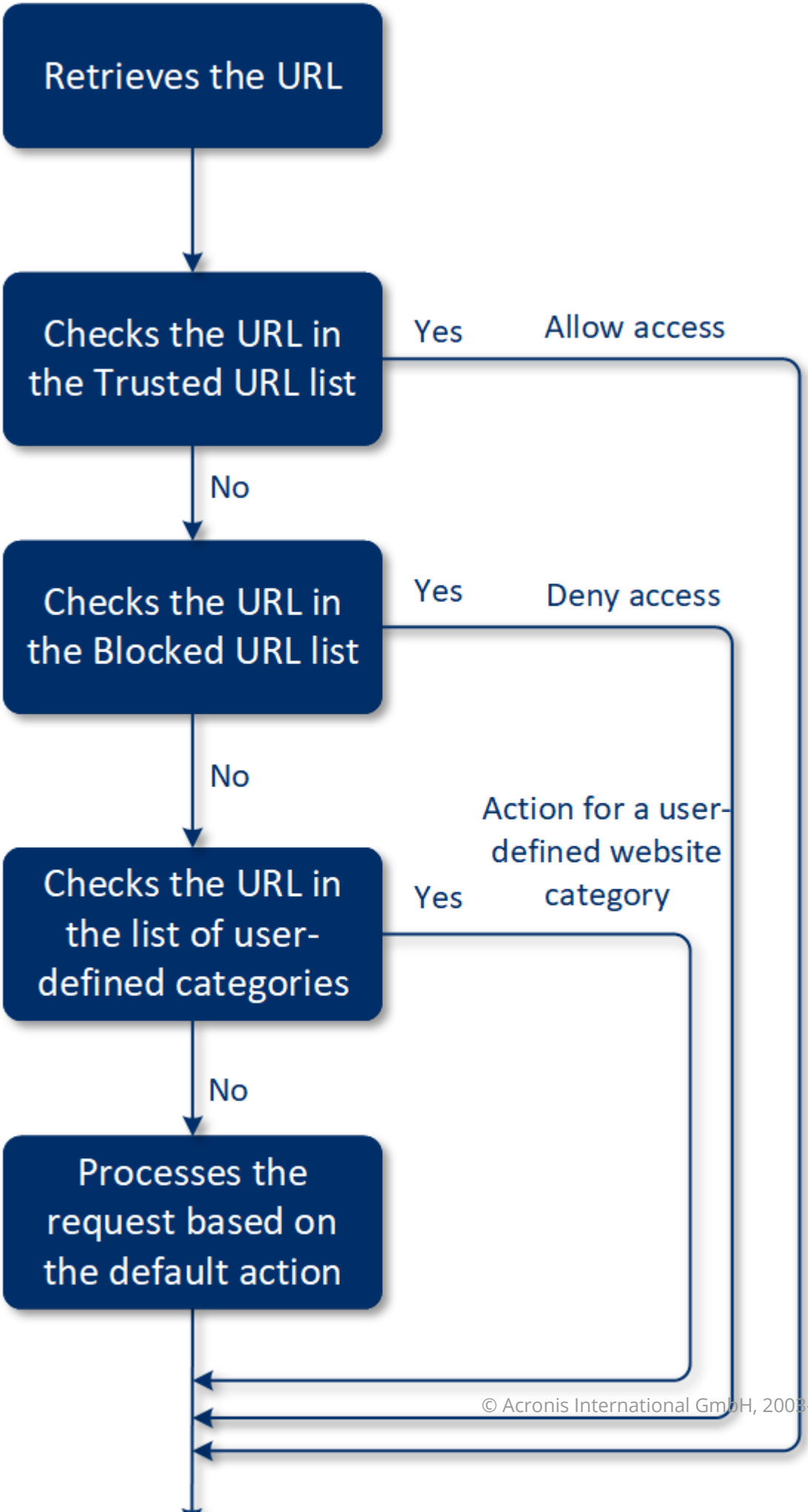
Funkcja Filtrowanie adresów URL wymaga do działania połączenia z Internetem.

Uwaga
Aby zapobiec potencjalnym problemom ze zgodnością kompilacji agenta ochrony 15.0.26692 (wersja C21.03 HF1) lub starszych, w przypadku wykrycia innego rozwiązania antywirusowego lub braku w systemie usługi Centrum zabezpieczeń systemu Windows funkcja Filtrowanie adresów URL zostanie automatycznie wyłączona.
W nowszych agentach ochrony problemy ze zgodnością zostały rozwiązane, w związku z czym usługa Filtrowanie adresów URL jest zawsze włączona zgodnie z zasadami.

Sposób działania

Użytkownik wpisuje w przeglądarce łącze URL. Kolektor przesyła to łącze do agenta ochrony. Agent uzyskuje adres URL, analizuje go, a następnie sprawdza wynik. Kolektor przekierowuje użytkownika do strony z komunikatem o dostępnych działaniach, aby umożliwić ręczne otwarcie żądanej strony.

© Acronis International GmbH, 2003-2024



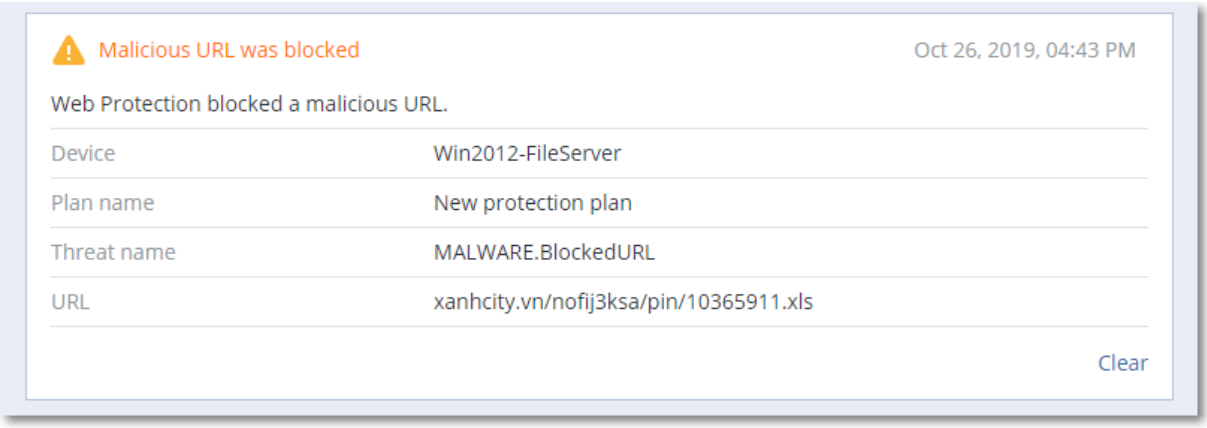
© Acronis International GmbH, 2003-2024

Proces konfiguracji modułu Filtrowanie adresów URL

Ogólnie rzecz biorąc, proces konfiguracji modułu Filtrowanie adresów URL obejmuje następujące działania:

1. Utwórz plan ochrony z włączonym modułem **Filtrowanie adresów URL**.
2. Określ ustawienia filtrowania adresów URL (patrz poniżej).
3. Przypisz plan ochrony do komputerów.

Aby sprawdzić zablokowane adresy URL, przejdź do sekcji **Monitorowanie** > **Alerty**.



Ustawienia modułu Filtrowanie adresów URL

W przypadku modułu Filtrowanie adresów URL można określić następujące ustawienia.

Dostęp do złośliwych witryn internetowych

Określ działanie, które ma zostać wykonane, gdy użytkownik spróbuje wyświetlić złośliwą witrynę internetową:

- **Tylko powiadom** — oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania służące wymuszeniu okupu.
- **Blokuj** — powoduje zablokowanie dostępu do złośliwej witryny internetowej. Użytkownik nie będzie mógł uzyskać dostępu do tej witryny internetowej i zostanie wygenerowany alert ostrzegawczy.
- **Zawsze pytaj użytkownika** — powoduje wyświetlenie pytania, czy witryna internetowa ma zostać mimo wszystko otwarta, czy użytkownik chce wrócić do poprzedniej strony.

Kategorie do filtrowania

Dostępne są 44 kategorie witryn internetowych, według których można konfigurować dostęp:

- **Pozwól** — zezwolenie na dostęp do witryn internetowych związanych z wybraną kategorią.
- **Odmów** — blokowanie dostępu do witryn internetowych związanych z wybraną kategorią.

© Acronis International GmbH, 2003-2024

Domyślnie są dozwolone wszystkie kategorie.

Pokaż wszystkie powiadomienia o zablokowanych adresach URL według kategorii — w przypadku włączenia tej opcji na pasku zadań będą wyświetlane wszelkie powiadomienia o zablokowanych adresach URL według kategorii. Jeśli witryna internetowa obejmuje kilka poddomen, to system generuje powiadomienia dotyczące również nich, w związku z czym liczba powiadomień może być duża.

W poniższej tabeli można znaleźć opisy kategorii:

	Kategoria witryny internetowej	Opis
1	**Reklamy**	Ta kategoria obejmuje domeny, których głównym celem jest wyświetlanie reklam.
2	**Tablice ogłoszeń**	Ta kategoria obejmuje fora, tablice dyskusyjne oraz strony internetowe typu „pytanie — odpowiedź”. Ta kategoria nie obejmuje części firmowych witryn internetowych, w których klienci zadają pytania.
3	**Osobiste witryny internetowe**	Ta kategoria obejmuje zarówno osobiste witryny internetowe, jak i wszelkiego rodzaju blogi: indywidualne, grupowe, a nawet firmowe. Blog to dziennik publikowany w sieci World Wide Web. Składa się on z wpisów („postów”) wyświetlanych zwykle w odwrotnej kolejności chronologicznej, tak że jako pierwszy pojawia się najnowszy post.
4	**Firmowe witryny internetowe**	To jest szeroka kategoria, obejmująca firmowe witryny internetowe, które zwykle nie należą do żadnej innej kategorii.
5	**Oprogramowanie komputerowe**	Ta kategoria obejmuje witryny internetowe udostępniające oprogramowanie komputerowe, zazwyczaj typu open source, freeware lub shareware. Może ona również obejmować niektóre sklepy z oprogramowaniem online.
6	**Leki**	Ta kategoria obejmuje witryny internetowe związane z lekami, alkoholami i papierosami/cygarami, w których są prowadzone dyskusje na temat stosowania lub sprzedaży (legalnych) leków i związanych z nimi akcesoriów, alkoholu bądź wyrobów tytoniowych. Należy pamiętać, że nielegalne substancje są uwzględniane w kategorii Narkotyki.
7	**Edukacja**	Ta kategoria obejmuje witryny internetowe należące do oficjalnych instytucji edukacyjnych, również spoza domeny .edu. Uwzględniono w niej również witryny edukacyjne, np. encyklopedie.
8	**Rozrywka**	Ta kategoria obejmuje witryny internetowe, które udostępniają informacje związane z działalnością artystyczną i muzeami, a także witryny internetowe z recenzjami i ocenami różnych dzieł, takich jak filmy, muzyka czy sztuka.
9	**Udostępnianie plików**	Ta kategoria obejmuje witryny internetowe służące do udostępniania

© Acronis International GmbH, 2003-2024

		plików, do których użytkownik może przesyłać pliki, by udostępniać je innym. Obejmuje ona również witryny służące do udostępniania torrentów oraz trackery torrentów.
10	**Finanse**	Ta kategoria obejmuje witryny internetowe należące do wszelkich banków z całego świata oferujących dostęp przez Internet. Należą do niej również niektóre unie kredytowe i inne instytucje finansowe. Jednak niektóre lokalne banki mogą nie być w niej ujęte.
11	**Gry hazardowe**	Ta kategoria obejmuje hazardowe witryny internetowe. Są to witryny typu „kasyno online" lub „loteria online", które zazwyczaj wymagają płatności, zanim użytkownik będzie mógł grać na pieniądze w ruletkę, pokera, blackjacka lub podobne gry online. Niektóre z nich są legalne, co oznacza, że jest szansa na wygraną, a niektóre fałszywe, co oznacza, że nie ma szans na wygraną. Rozpoznawane są również witryny z „niezawodnymi sposobami" na zarabianie pieniędzy na hazardzie i loteriach online.
12	**Gry**	Ta kategoria obejmuje witryny internetowe udostępniające gry online, zazwyczaj oparte na apletach Adobe Flash lub JAVA. Nie ma znaczenia, czy gra jest darmowa, czy wymaga abonamentu, jednak witryny internetowe typu kasyno są wykrywane w kategorii Gry hazardowe. Oto czego ta kategoria nie obejmuje: • Oficjalne witryny internetowe firm produkujących gry wideo (pod warunkiem, że nie produkują one gier online) • Witryny internetowe będące miejscami dyskusji o grach • Witryny internetowe, z których można pobierać gry działające w trybie offline (niektóre z nich znajdują się w kategorii Nielegalne pobieranie plików). • Gry, które wymagają od użytkownika pobrania i uruchomienia pliku wykonywalnego, takie jak World of Warcraft — można temu zapobiec za pomocą różnych środków, na przykład zapory.
13	**Administracja publiczna**	Ta kategoria obejmuje witryny internetowe administracji publicznej, w tym urzędów, państwowych instytucji i ambasad.
14	**Hakowanie**	Ta kategoria obejmuje witryny internetowe, które udostępniają narzędzia, artykuły i platformy dyskusyjne dla hakerów. Obejmuje ona również witryny oferujące exploity do popularnych platform, które ułatwiają hakowanie kont na Facebooku lub Gmailu.
15	**Nielegalne działania**	To jest szeroka kategoria związana z nienawiścią, przemocą i rasizmem, umożliwiająca blokowanie następujących rodzajów witryn internetowych: • Witryny należące do organizacji terrorystycznych • Witryny zawierające treści rasistowskie lub ksenofobiczne • Witryny będące miejscami dyskusji o agresywnych sportach i/lub promujące przemoc

© Acronis International GmbH, 2003-2024

16	**Zdrowie i fitness**	Ta kategoria obejmuje witryny internetowe instytucji opieki zdrowotnej oraz dotyczące profilaktyki i leczenia chorób, witryny udostępniające informacje lub produkty związane z odchudzaniem, żywieniem, sterydami, anabolikami czy hormonami wzrostu, a także witryny z informacjami o operacjach plastycznych.
17	**Hobby**	Ta kategoria obejmuje witryny internetowe, które oferują materiały i produkty związane z działaniami wykonywanymi na ogół w czasie wolnym od pracy, takimi jak kolekcjonerstwo, sztuka i rzemiosło czy jazda na rowerze.
18	**Hosting witryn internetowych**	Ta kategoria obejmuje bezpłatne i komercyjne usługi hostingowe, które umożliwiają prywatnym użytkownikom oraz firmom i instytucjom tworzenie i publikowanie stron internetowych.
19	**Nielegalne pobieranie plików**	Ta kategoria obejmuje witryny internetowe umożliwiające piractwo oprogramowania, takie jak: • Witryny do śledzenia peer-to-peer (BitTorrent, emule, DC++) znane z ułatwiania rozpowszechniania treści chronionych prawami autorskimi bez zgody właścicieli praw autorskich • Witryny internetowe i tablice ogłoszeń związane z warezami (spiratowanym oprogramowaniem komercyjnym) • Witryny internetowe udostępniające użytkownikom cracki, generatory kluczy i numery seryjne umożliwiające nielegalne korzystanie z oprogramowania. Niektóre z tych witryn internetowych mogą też być wykrywane jako pornografia lub alkohol/papierosy, ponieważ często w celach zarobkowych są w nich zamieszczane reklamy pornografii lub alkoholu.
20	**Komunikatory i czaty**	Ta kategoria obejmuje komunikatory internetowe i czaty, które umożliwiają rozmawianie w czasie rzeczywistym. W jej ramach będą wykrywane również witryny yahoo.com i gmail.com, ponieważ obie mają wbudowane komunikatory internetowe.
21	**Oferty pracy**	Ta kategoria obejmuje witryny internetowe z tablicami ogłoszeń o pracę albo reklamami związanymi z ofertami pracy i możliwościami rozwoju kariery, a także agregatory takich usług. Nie obejmuje ona agencji rekrutacyjnych ani stron „ofert pracy" w zwykłych firmowych witrynach internetowych.
22	**Treści dla osób dojrzałych**	Ta kategoria obejmuje treści, które zostały oznaczone przez twórcę witryny internetowej jako wymagające dojrzałej publiczności. Obejmuje ona szeroką gamę witryn internetowych: od poświęconych książce Kama Sutra i edukacji seksualnej po twardą pornografię.
23	**Narkotyki**	Ta kategoria obejmuje witryny internetowe udostępniające informacje o rekreacyjnych i nielegalnych narkotykach. Obejmuje ona również witryny dotyczące produkcji lub uprawy narkotyków.

© Acronis International GmbH, 2003-2024

24	**Wiadomości**	Ta kategoria obejmuje witryny internetowe z informacjami w formie tekstowej i wideo. W kategorii tej próbuje się uwzględniać wszelkie — zarówno globalne, jak i lokalne — serwisy informacyjne, jednak niektóre małe, lokalne serwisy informacyjne mogą nie być nią objęte.
25	**Randki online**	Ta kategoria obejmuje randkowe witryny internetowe — płatne i bezpłatne — w których użytkownicy mogą wyszukiwać inne osoby według wybranych kryteriów. Mogą też umieszczać własne profile, aby inni mogli je wyszukiwać. Ta kategoria obejmuje zarówno darmowe, jak i płatne witryny randkowe. Ponieważ większość popularnych portali społecznościowych może pełnić funkcję witryn randkowych, niektóre z nich, np. Facebook, również są wykrywane w tej kategorii. Warto korzystać z tej kategorii w połączeniu z kategorią Portale społecznościowe.
26	**Płatności online**	Ta kategoria obejmuje witryny internetowe obsługujące płatności online lub przelewy pieniężne. Wykrywane są w niej popularne witryny obsługujące płatności, takie jak PayPal czy Moneybookers. Ponadto w zwykłych witrynach heurystycznie wykrywane są strony z monitami o podanie danych karty kredytowej, co pozwala na wykrycie ukrytych, nieznanych lub nielegalnych sklepów internetowych.
27	**Udostępnianie zdjęć**	Ta kategoria obejmuje witryny internetowe, których głównym celem jest umożliwienie użytkownikom zamieszczania i udostępniania zdjęć.
28	**Sklepy online**	Ta kategoria obejmuje znane sklepy internetowe. Witryna internetowa jest uznawana za sklep internetowy, jeśli sprzedaje towary lub usługi online.
29	**Pornografia**	Ta kategoria obejmuje witryny internetowe zawierające treści erotyczne i pornograficzne. Obejmuje ona zarówno płatne, jak i bezpłatne witryny ze zdjęciami, opowiadaniami i filmami. Wykrywane są też treści pornograficzne w witrynach z różnorodną zawartością.
30	**Portale**	Ta kategoria obejmuje witryny internetowe, które agregują informacje z wielu źródeł oraz różnych domen i które zwykle udostępniają takie funkcje jak wyszukiwarki, poczta e-mail oraz informacje o wydarzeniach lub dotyczące rozrywki.
31	**Radio**	Ta kategoria obejmuje witryny internetowe, które oferują strumieniową transmisję muzyki — od internetowych stacji radiowych po witryny udostępniające treści audio na żądanie (bezpłatne lub płatne).
32	**Religia**	Ta kategoria obejmuje witryny internetowe promujące religię lub sektę. Obejmuje ona również fora dyskusyjne związane z jedną lub wieloma religiami.
33	**Wyszukiwarki**	Ta kategoria obejmuje wyszukiwarki internetowe, takie jak Google, Yahoo i Bing.
34	**Portale**	Ta kategoria obejmuje portale społecznościowe, np. MySpace.com,

© Acronis International GmbH, 2003-2024

	społecznościowe	Facebook.com, Bebo.com itp. Jednak wyspecjalizowane portale społecznościowe, takie jak YouTube.com, będą wymieniane w kategorii Filmy/zdjęcia.
35	**Sport**	Ta kategoria obejmuje witryny internetowe, które oferują informacje sportowe, wiadomości i instruktaże.
36	**Samobójstwa**	Ta kategoria obejmuje witryny internetowe promujące samobójstwa i nawołujące do nich. Nie obejmuje ona klinik profilaktyki samobójstw.
37	**Tabloidy**	Ta kategoria dotyczy głównie witryn internetowych z miękką pornografią i plotkami o gwiazdach. Wiele witryn internetowych z tabloidowymi wiadomościami może mieć wymienione tu podkategorie. W tej kategorii również wykrywanie jest oparte na heurystyce.
38	**Marnotrawstwo czasu**	Ta kategoria obejmuje witryny internetowe, w których użytkownicy spędzają mnóstwo czasu. Mogą się niej znaleźć witryny z innych kategorii, na przykład portale społecznościowe lub witryny rozrywkowe.
39	**Podróże**	Ta kategoria obejmuje witryny internetowe, w których są prezentowane oferty wyjazdów turystycznych i sprzętu turystycznego, a także opinie i oceny dotyczące celów podróży.
40	**Wideo**	Ta kategoria obejmuje witryny internetowe, w których są dostępne filmy lub zdjęcia przesyłane przez użytkowników bądź dostarczane przez różnych dostawców treści. Dotyczy to na przykład witryn YouTube, Metacafe i Google Video, a także witryn ze zdjęciami, takich jak Picasa czy Flickr. Będą wykrywane również filmy wideo osadzone w innych witrynach lub blogach.
41	**Brutalne kreskówki**	Ta kategoria obejmuje witryny internetowe omawiające, udostępniające i oferujące brutalne kreskówki lub mangi, które mogą być nieodpowiednie dla osób nieletnich ze względu na przemoc, wulgaryzmy lub treści seksualne. Kategoria ta nie obejmuje witryn udostępniających kreskówki z głównego nurtu, takich jak „Tom i Jerry”.
42	**Broń**	Ta kategoria obejmuje witryny internetowe dotyczące sprzedaży lub wymiany, produkcji bądź użytkowania broni. Uwzględniane są tu również witryny z wyposażeniem myśliwskim oraz dotyczące korzystania z wiatrówek i pistoletów na śrut BB, a także broni używanej w walce wręcz.
43	**E-mail**	Ta kategoria obejmuje witryny internetowe, które udostępniają pocztę e-mail jako aplikację internetową.
44	**Serwer proxy WWW**	Ta kategoria obejmuje witryny internetowe udostępniające usługę serwera proxy WWW. Chodzi tu o witryny typu „przeglądarka w przeglądarce”: gdy użytkownik chcesz otworzyć stronę internetową, wpisuje jej adres URL w formularzu i klika „Prześlij” („Submit”). Witryna serwera proxy WWW pobiera daną stronę i wyświetla ją w przeglądarce użytkownika. Powody do wykrywania tego typu ruchu (i ewentualnej konieczności jego

© Acronis International GmbH, 2003-2024

		blokowania): • Anonimowe przeglądanie. Ponieważ żądania wysyłane do docelowego serwera WWW przychodzą z serwera proxy, widoczny jest tylko jego adres IP, więc jeśli administratorzy serwera spróbują wyśledzić trasę użytkownika, trop urwie się na serwerze proxy, który nie musi mieć dzienników niezbędnych do zlokalizowania inicjującego sesję użytkownika. • Spoofing lokalizacji. Adresy IP użytkowników często są używane do profilowania usługi według lokalizacji źródłowej (niektóre krajowe strony administracji publicznej mogą być dostępne tylko z lokalnych adresów IP), więc skorzystanie z takiej usługi może użytkownikowi pomóc w sfałszowaniu swojej rzeczywistej lokalizacji. • Dostęp do wzbronionych treści. Jeśli zostanie użyty prosty filtr adresów URL, będzie on wykrywał tylko adresy serwera proxy WWW, a nie adresy rzeczywistych serwerów odwiedzanych przez użytkownika. • Uniknięcie monitorowania przez pracodawcę. W firmie może obowiązywać zasada monitorowania użytkowania Internetu przez pracowników. Uzyskując dostęp do stron za pośrednictwem serwera proxy WWW, użytkownik może sprawić, że monitorowania nie zapewni firmie rzetelnych informacji. Ponieważ zestaw SDK analizuje stronę HTML (jeśli będzie dostępna), a nie tylko adres URL, w przypadku niektórych kategorii zestaw SDK nadal będzie w stanie rozpoznać wyświetlane treści. Jednak w przypadku innych powodów problemów nie da się uniknąć tylko przez zastosowanie zestawu SDK.

Wykluczenia adresów URL

Adresy URL, które są znane jako bezpieczne, można dodać do listy zaufanych domen. Adresy URL, które stanowią zagrożenie, można dodać do listy blokowanych domen.

Aby wskazać adresy URL, które zawsze będą traktowane jako zaufane lub blokowane

1. W module Filtrowanie adresów URL planu ochrony kliknij **Wykluczenia adresów URL**.
   Zostanie otwarte okno **Wykluczenia adresów URL**.
   Zostaną wyświetlone następujące opcje:

Elementy zaufane — kliknij **Dodaj**, aby wybrać jedną z dostępnych opcji:

- **Domena** — w przypadku wybrania tej opcji zostanie otwarte okno **Dodaj domenę**.
  - W polu **Domena** wprowadź każdą domenę w osobnym wierszu. W polu **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów zaufanych.
- **Proces** — w przypadku wybrania tej opcji zostanie wyświetlone okno **Dodaj proces**.
  - W polu **Proces** wprowadź w osobnych wierszach ścieżki do poszczególnych procesów. W sekcji **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów zaufanych.

Elementy blokowane — kliknij **Dodaj**. Zostanie wyświetlone okno **Dodaj domenę**.

© Acronis International GmbH, 2003-2024

W polu **Domena** wprowadź każdą domenę w osobnym wierszu. W polu **Opis** wprowadź krótki opis, aby dało się rozpoznać zmianę na liście elementów blokowanych.

Uwaga
Obsługiwane są lokalne ścieżki sieciowe. Na przykład \\localhost\ścieżkafolderu\plik.exe.

Opis

W polu **Opis** można wpisać uwagi na temat wykluczeń dodanych do listy wykluczeń adresów URL. Oto garść podpowiedzi dotyczących ewentualnych uwag:

- Przyczyny i cele wykluczenia.
- Sygnatury czasowe.

Jeśli w jednym wpisie dodano więcej niż jeden element, można zarejestrować tylko 1 komentarz dotyczący wszystkich tych elementów.

Oprogramowanie Microsoft Defender Antivirus i Microsoft Security Essentials

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Moduł Microsoft Defender Antivirus

Microsoft Defender Antivirus to wbudowany komponent ochrony antywirusowej udostępniany wraz z systemem Microsoft Windows, począwszy od wersji Windows 8.

Program Microsoft Defender Antivirus (WDA) pozwala na skonfigurowanie zasad zabezpieczeń programu Microsoft Defender Antivirus i monitorowanie ich statusu za pomocą konsoli Cyber Protect.

Moduł ten ma zastosowanie do obciążeń, w których zainstalowano oprogramowanie Microsoft Defender Antivirus.

Microsoft Security Essentials

Microsoft Security Essentials to wbudowany komponent ochrony antywirusowej udostępniany wraz z systemem Microsoft Windows, począwszy od wersji Windows 8.

Program Microsoft Security Essentials umożliwia skonfigurowanie zasad zabezpieczeń programu Microsoft Security Essentials i monitorowanie ich statusu za pomocą konsoli Cyber Protect.

Moduł ten ma zastosowanie do obciążeń, w których zainstalowano program Microsoft Security Essentials.

© Acronis International GmbH, 2003-2024

Ustawienia programu Microsoft Security Essentials są podobne do ustawień programu Microsoft Defender Antivirus, ale w ich przypadku nie można skonfigurować ochrony w czasie rzeczywistym ani zdefiniować wykluczeń za pomocą konsoli Cyber Protect.

Zaplanuj skanowanie

Określ harmonogram planowanych operacji skanowania.

Tryb skanowania:

- **Pełne** — pełne sprawdzenie wszystkich plików i folderów oprócz elementów skanowanych podczas szybkiego skanowania. Takie skanowanie wymaga więcej zasobów komputera niż szybkie skanowanie.
- **Szybkie** — szybkie sprawdzenie procesów w pamięci oraz folderów, w których zwykle wykrywa się złośliwe oprogramowanie. Takie skanowanie wymaga mniej zasobów komputera niż pełne skanowanie.

Należy określić godzinę i dzień tygodnia, w którym będzie wykonywane.

Codziennie szybkie skanowanie — należy określić godzinę codziennego szybkiego skanowania.

W zależności od potrzeb można włączyć jedną z opcji:

Rozpocznij zaplanowane skanowanie, gdy komputer jest włączony, ale nie jest używany

Przed zaplanowanym skanowaniem sprawdź dostępność najnowszych definicji wirusów i oprogramowania szpiegowskiego

Ogranicz obciążenie procesora podczas skanowania do

Dodatkowe informacje na temat ustawień modułu Microsoft Defender Antivirus można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings.

Czynności domyślne

Zdefiniuj domyślne działania, które mają być wykonywane w przypadku wykrytych zagrożeń o różnych poziomach ważności:

- **Wyczyść** — wykryte złośliwe oprogramowanie zostaje wyczyszczone z obciążenia.
- **Kwarantanna** — wykryte złośliwe oprogramowanie zostaje umieszczone w folderze kwarantanny, ale nie usunięte.
- **Usuń** — wykryte złośliwe oprogramowanie zostaje usunięte z obciążenia.
- **Pozwól** — wykryte złośliwe oprogramowanie nie zostaje usunięte ani poddane kwarantannie.
- **Określone przez użytkownika** — użytkownik otrzymuje monit o określenie, co należy zrobić z wykrytym złośliwym oprogramowaniem.
- **Brak czynności** — żadne czynności nie są podejmowane.
- **Blokuj** — wykryte złośliwe oprogramowanie zostaje zablokowane.

© Acronis International GmbH, 2003-2024

Dodatkowe informacje na temat domyślnych ustawień czynności modułu Microsoft Defender Antivirus można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings

Ochrona w czasie rzeczywistym

Włącz opcję **Ochrona w czasie rzeczywistym**, aby aktywować wykrywanie złośliwego oprogramowania oraz blokowanie jego instalacji lub uruchamiania w obciążeniach.

Skanuj wszystkie pobierane pliki — w przypadku zaznaczenia tej opcji będą skanowane wszystkie pobierane pliki i załączniki.

Włącz monitorowanie zachowań — w przypadku zaznaczenia tej opcji zostanie włączone monitorowanie zachowań.

Skanuj pliki sieciowe — w przypadku zaznaczenia tej opcji będą skanowane pliki sieciowe.

Zezwól na pełne skanowanie zamapowanych dysków sieciowych — w przypadku zaznaczenia tej opcji będą w pełni skanowane dyski sieciowe.

Zezwól na skanowanie poczty e-mail — w przypadku zaznaczenia tej opcji będą skanowane pliki skrzynki pocztowej, w zależności od ich formatu, w celu analizowania treści i załączników wiadomości e-mail.

Dodatkowe informacje na temat ustawień ochrony w czasie rzeczywistym modułu Microsoft Defender Antivirus można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings

Zaawansowany

Określ zaawansowane ustawienia skanowania:

- **Skanuj pliki archiwum** — powoduje przeskanowanie również plików archiwów, takich jak .zip czy .rar.
- **Skanuj dyski wymienne** — powoduje przeskanowanie dysków wymiennych w ramach pełnego skanowania.
- **Utwórz punkt przywracania systemu** — czasem ważny plik lub wpis w rejestrze może zostać usunięty jako „fałszywy alarm”, a wówczas można go odzyskać z punktu przywracania.
- **Usuń pliki z kwarantanny po** — umożliwia określenie, po jakim czasie pliki poddane kwarantannie zostaną usunięte.
- **Automatycznie wysyłaj próbki plików, gdy jest wymagana dodatkowa analiza:**
  - **Zawsze monituj** — przed wysłaniem pliku pojawi się monit o potwierdzenie.
  - **Automatycznie wysyłaj bezpieczne próbki** — większość próbek będzie wysyłanych automatycznie, z wyjątkiem plików, które mogą zawierać dane osobowe. Takie pliki będą wymagały dodatkowego potwierdzenia.
  - **Automatycznie wysyłaj wszystkie próbki** — wszystkie próbki będą wysyłane automatycznie.

© Acronis International GmbH, 2003-2024

- **Wyłącz interfejs programu antywirusowego Windows Defender** — w przypadku zaznaczenia tej opcji interfejs użytkownika programu antywirusowego Windows Defender nie będzie dostępny dla użytkownika. Zasadami zabezpieczeń programu WDA można zarządzać w konsoli Cyber Protect.
- **MAPS (Microsoft Active Protection Service)** — społeczność online, która pomaga wybrać sposób reagowania na potencjalne zagrożenia.
  - **Nie chcę dołączać do MAPS** — do firmy Microsoft nie będą wysyłane żadne informacje o wykrytym oprogramowaniu.
  - **Podstawowe członkostwo** — do firmy Microsoft będą wysyłane podstawowe informacje o wykrytym oprogramowaniu.
  - **Zaawansowane członkostwo** — do firmy Microsoft będą wysyłane szczegółowe informacje o wykrytym oprogramowaniu.

  Więcej informacji można znaleźć pod adresem https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/

Dodatkowe informacje na temat ustawień zaawansowanych modułu Microsoft Defender Antivirus można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings

Wykluczenia

Ze skanowania można wykluczyć następujące pliki i foldery:

- **Procesy** — ze skanowania zostanie wykluczony każdy plik, z którego odczytuje lub w którym zapisuje zdefiniowany proces. Należy zdefiniować pełną ścieżkę do pliku wykonywalnego procesu.
- **Pliki i foldery** — ze skanowania zostaną wykluczone wskazane pliki i foldery. Należy zdefiniować pełną ścieżkę do folderu lub pliku lub zdefiniować rozszerzenie pliku.

Dodatkowe informacje na temat ustawień wykluczeń modułu Microsoft Defender Antivirus można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings

Zarządzanie zaporą

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Zarządzanie zaporą umożliwia łatwe konfigurowanie ustawień zapory dla chronionych obciążeń.

Te funkcje w usłudze Cyber Protect są zapewniane przez wbudowany składnik zapory Microsoft Defender systemu Microsoft Windows. Zapora Microsoft Defender blokuje nieautoryzowany ruch sieciowy wpływający do obciążeń lub z nich wypływający.

© Acronis International GmbH, 2003-2024

Zarządzanie zaporą ma zastosowanie do obciążeń, w których zainstalowano zaporę Microsoft Defender.

Obsługiwane systemy operacyjne Windows

Jeśli chodzi o zarządzanie zaporą, obsługiwane są następujące systemy operacyjne Windows:

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

System Windows Server nie jest obsługiwany.

Włączanie i wyłączanie zarządzania zaporą

Podczas tworzenia planu ochrony można włączyć zarządzanie zaporą. Można też zmienić istniejący już plan ochrony w celu włączenia lub wyłączenia zarządzania zaporą.

Aby włączyć lub wyłączyć zarządzanie zaporą

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wykonaj jedną z następujących czynności, aby otworzyć panel planu ochrony:
   - Jeśli chcesz utworzyć nowy plan ochrony, wybierz komputer, który ma być chroniony, a następnie kliknij **Chroń** i **Utwórz plan**.
   - Jeśli chcesz zmienić już istniejący plan ochrony, wybierz chroniony komputer, kliknij **Chroń**, kliknij wielokropek (...) obok nazwy planu ochrony, a następnie kliknij **Edytuj**.
3. Na panelu planu ochrony przejdź do obszaru **Zarządzanie zaporą** i włącz lub wyłącz przełącznik **Zarządzanie zaporą**.
4. Aby zastosować wprowadzone zmiany, wykonaj jedną z następujących czynności:
   - W przypadku tworzenia planu kliknij **Utwórz**.
   - W przypadku edytowania planu kliknij **Zapisz**.

Status zapory Microsoft Defender w obszarze **Zarządzanie zaporą** panelu planu ochrony jest wyświetlany jako **Włączony** lub **Wyłączony** w zależności od tego, czy włączono lub wyłączono zarządzanie zaporą.

Panel planu ochrony można też otworzyć z poziomu karty Zarządzanie.Funkcja ta jednak jest niedostępna w niektórych wersjach usługi Cyber Protection.

Kwarantanna

Kwarantanna to specjalny, odizolowany folder na dysku twardym komputera, w którym są umieszczane podejrzane pliki wykryte przez moduł Ochrona przed wirusami i złośliwym

© Acronis International GmbH, 2003-2024

oprogramowaniem w celu zapobieżenia dalszemu rozprzestrzenianiu się zagrożeń.

Kwarantanna pozwala na przeglądanie podejrzanych oraz potencjalnie niebezpiecznych plików ze wszystkich komputerów i decydowanie o ich usunięciu lub przywróceniu. Pliki poddane kwarantannie są automatycznie usuwane w przypadku usunięcia komputera z systemu.

Jak pliki trafiają do folderu kwarantanny?

1. Użytkownik konfiguruje plan ochrony i definiuje domyślne działanie dotyczące zainfekowanych plików — umieszczenie ich w kwarantannie.
2. Podczas skanowania zaplanowanego lub wykonywanego przy dostępie system wykrywa złośliwe pliki i umieszcza je w bezpiecznym folderze, czyli w kwarantannie.
3. System aktualizuje listę kwarantanny na poszczególnych komputerach.
4. Pliki są automatycznie czyszczone z folderu kwarantanny po upływie czasu określonego za pomocą ustawienia **Usuń pliki z kwarantanny po** w planie ochrony.

Zarządzanie plikami poddanymi kwarantannie

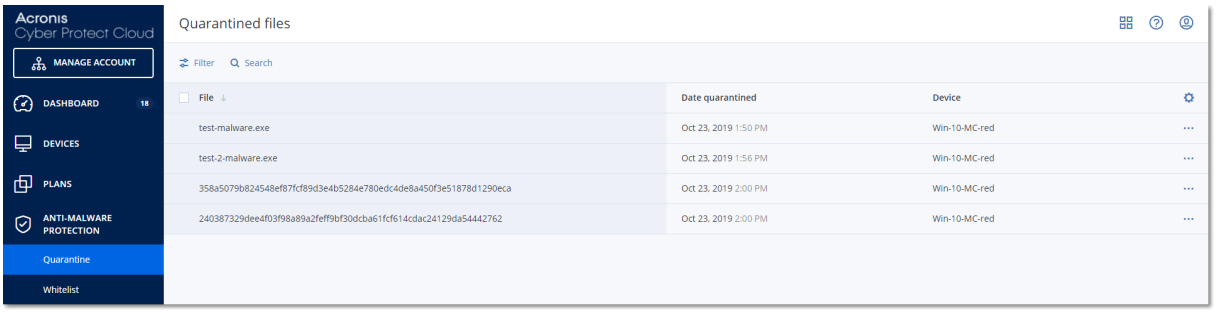
Aby zarządzać plikami poddanymi kwarantannie, przejdź do sekcji **Ochrona antywirusowa** > **Kwarantanna**. Zostanie wyświetlona lista z plikami poddanymi kwarantannie ze wszystkich komputerów.

Nazwa	Opis
Plik	Nazwa pliku.
Data rozpoczęcia kwarantanny	Data i godzina umieszczenia pliku w kwarantannie.
Urządzenie	Urządzenie, na którym znaleziono zainfekowany plik.
Nazwa zagrożenia	Nazwa zagrożenia.
Plan ochrony	Plan ochrony, zgodnie z którym podejrzany plik został umieszczony w kwarantannie.

W odniesieniu do plików poddanych kwarantannie można wykonać dwa działania:

- **Usuń** — trwałe usunięcie pliku poddanego kwarantannie ze wszystkich komputerów. Można usunąć wszystkie pliki z tym samym skrótem pliku. Można przywrócić wszystkie pliki z tym samym skrótem pliku. Pogrupuj pliki według skrótów, zaznacz odpowiednie pliki, a następnie je usuń.
- **Przywróć** — przywrócenie pliku poddanego kwarantannie do pierwotnej lokalizacji bez żadnych modyfikacji. Jeśli w pierwotnej lokalizacji jest już plik o danej nazwie, zostanie on zastąpiony przywracanym plikiem. Należy pamiętać, że przywrócony plik zostanie dodany do listy dozwolonych i będzie pomijany podczas kolejnych operacji skanowania antywirusowego.

© Acronis International GmbH, 2003-2024



Lokalizacja kwarantanny na komputerach

Domyślna lokalizacja plików poddanych kwarantannie to:

- W przypadku komputera z systemem Windows: `%programdata%\Acronis\NGMP\quarantine`
- W przypadku komputera Mac: `/Library/Application Support/Acronis/NGMP/quarantine`
- W przypadku komputera z systemem Linux: `/var/lib/Acronis/NGMP/quarantine`

Magazyn kwarantanny jest objęty ochroną własną dostawcy usługi.

Samoobsługowy niestandardowy folder na żądanie

W przypadku obciążenia można wybrać foldery niestandardowe i je skanować bezpośrednio z menu kontekstowego.

Aby uzyskać dostęp funkcji skanowania przy użyciu opcji Cyber Protect z menu kontekstowego

W przypadku obciążeń, dla których w planie ochrony włączono funkcję Ochrona przed wirusami i złośliwym oprogramowaniem, kliknij prawym przyciskiem myszy pliki/foldery, które mają zostać przeskanowane.

Uwaga
Ta opcja jest dostępna wyłącznie dla administratorów danego obciążenia.

Firmowa biała lista

Rozwiązanie antywirusowe może rozpoznawać dozwolone aplikacje firmowe jako podejrzane. Aby zapobiec fałszywym alarmom podczas wykrywania, dodaje się zaufane aplikacje do białej listy ręcznie, a to jest czasochłonne zajęcie.

Uwaga
Firmowa biała lista nie ma wpływu na skanowanie kopii zapasowych pod kątem złośliwego oprogramowania.

Usługa Cyber Protection może zautomatyzować ten proces: kopie zapasowe są skanowane przez moduł Ochrona przed wirusami i złośliwym oprogramowaniem, a skanowane dane są analizowane w celu przeniesienia takich aplikacji na białą listę, co zapobiega fałszywym alarmom podczas

© Acronis International GmbH, 2003-2024

wykrywania. Ponadto ogólnofirmowa biała lista poprawia wydajność kolejnych operacji skanowania pod kątem złośliwego oprogramowania.

Biała lista jest tworzona dla każdego klienta z osobna i opiera się tylko na jego danych.

Białą listę można włączać lub wyłączać. Gdy jest wyłączona, dodawane do niej pliki będą tymczasowo ukrywane.

Uwaga
Uprawnienia do konfigurowania białej listy i zarządzania nią mają tylko konta z rolą administratora (np. administrator usługi Cyber Protection, administrator firmy, administrator partnera działający w imieniu administratora firmy, administrator jednostki). Ta funkcja jest niedostępna w przypadku kont administratorów w trybie tylko do odczytu i kont użytkowników.

Automatyczne dodawanie pozycji do białej listy

1. Uruchom skanowanie kopii zapasowych w chmurze na co najmniej dwóch komputerach. Można to zrobić za pomocą planów skanowania kopii zapasowych.
2. Następnie w ustawieniach białej listy włącz przełącznik **Automatyczne generowanie białej listy**.

Ręczne dodawanie pozycji do białej listy

Nawet jeśli przełącznik **Automatyczne generowanie białej listy** jest wyłączony, można ręcznie dodać pliki do białej listy.

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona przed złośliwym oprogramowaniem** > **Biała lista**.
2. Kliknij **Dodaj plik**.
3. Określ ścieżkę do pliku i kliknij **Dodaj**.

Dodawanie plików poddanych kwarantannie do białej listy

Do białej listy można dodawać pliki, które zostały poddane kwarantannie.

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona przed złośliwym oprogramowaniem** > **Kwarantanna**.
2. Wybierz plik poddany kwarantannie i kliknij **Dodaj do białej listy**.

Ustawienia białej listy

W przypadku włączenia przełącznika **Automatyczne generowanie białej listy** trzeba określić jeden z następujących poziomów ochrony heurystycznej:

- **Niski**
  — firmowe aplikacje zostaną dodane do białej listy dopiero po upływie dłuższego czasu i przeprowadzeniu kontroli. Takie aplikacje są uznawane za bardziej zaufane. Strategia ta jednak

© Acronis International GmbH, 2003-2024

zwiększa prawdopodobieństwo fałszywych alarmów podczas wykrywania. Kryteria uznania pliku za czysty i zaufany są wysokie.

- **Domyślne**
  — firmowe aplikacje będą dodawane do białej listy zgodnie z zalecanym poziomem ochrony w celu ograniczenia ewentualnych fałszywych alarmów podczas wykrywania. Kryteria uznania pliku za czysty i zaufany są średnie.
- **Wysoki**
  — firmowe aplikacje będą szybciej dodawane do białej listy, aby zmniejszyć liczbę ewentualnych fałszywych alarmów podczas wykrywania. Nie oznacza to jednak gwarancji niezainfekowania oprogramowania — później może ono zostać uznane za podejrzane lub za złośliwe oprogramowanie. Kryteria uznania pliku za czysty i zaufany są niskie.

Wyświetlanie szczegółowych informacji na temat pozycji z białej listy

Kliknięcie pozycji na białej liście umożliwia wyświetlenie dodatkowych informacji na jej temat i przeanalizowanie jej online.

Jeśli nie masz pewności co do dodanej pozycji, możesz ją sprawdzić w analizatorze VirusTotal. Jeśli klikniesz **Sprawdź w ramach VirusTotal**, witryna przeanalizuje podejrzane pliki i adresy URL pod kątem różnego typu złośliwego oprogramowania, korzystając ze skrótu pliku dodanej pozycji. Skrót można sprawdzić w ciągu **Skrót pliku (MD5)**.

Wartość **Komputery** reprezentuje liczbę komputerów, na których znaleziono taki skrót podczas skanowania kopii zapasowych. Wartość ta jest wypełniana tylko wtedy, gdy dana pozycja pochodzi ze skanowania kopii zapasowych lub kwarantanny. Jeśli plik został dodany do białej listy ręcznie, to pole pozostaje puste.

Skanowanie antywirusowe kopii zapasowych

Za pomocą funkcji skanowania antywirusowego można sprawdzić, czy kopie zapasowe są wolne od złośliwego oprogramowania, i w ten sposób zapobiec odzyskaniu zainfekowanych plików. Skanowanie antywirusowe jest wykonywane przez agenta w chmurze, który znajduje się w centrum danych Cyber Protection, i do wykonania tej operacji nie są używane żadne lokalne zasoby obliczeniowe.

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Aby przeprowadzić skanowanie antywirusowe, należy skonfigurować plan skanowania kopii zapasowych. Dodatkowe informacje o tym, jak to zrobić, można znaleźć w sekcji "Plany skanowania kopii zapasowych" (s. 247).

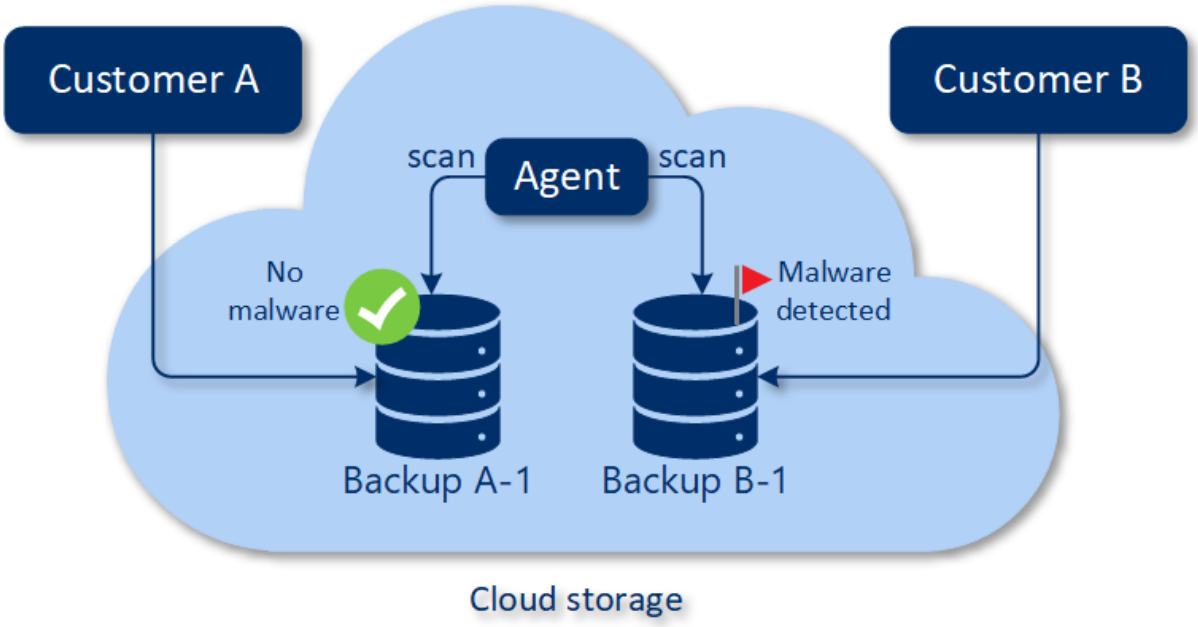
Każdy plan skanowania kopii zapasowych tworzy zadanie skanowania dla agenta w chmurze i dodaje to zadanie do kolejki (jest jedna kolejka na centrum danych). Zadania skanowania są przetwarzane według ich kolejności w kolejce. Czas skanowania zależy od wielkości kopii zapasowej.

© Acronis International GmbH, 2003-2024

To dlatego między utworzeniem planu skanowania kopii zapasowych a ukończeniem skanowania występuje pewne opóźnienie.

Kopie zapasowe wybrane do skanowania mogą się znajdować w jednym z następujących stanów:

- Nie przeskanowano
- Brak złośliwego oprogramowania
- Wykryto złośliwe oprogramowanie



Wyniki skanowania kopii zapasowych można sprawdzić w widżecie **Szczegóły skanowania kopii zapasowej (zagrożenia)**. Znajduje się on w konsoli Cyber Protect na karcie **Monitorowanie** > **Przegląd**.

Ograniczenia

- Skanowanie antywirusowe jest obsługiwane tylko w przypadku kopii zapasowych typu **Cały komputer** lub **Dyski/woluminy** utworzonych w odniesieniu do następujących obciążeń:
  - Komputery z systemem Windows, na których jest zainstalowany agent ochrony.
  - Maszyny wirtualne z systemem Windows, których kopie zapasowe są tworzone na poziomie hiperwizorów (bezagentowe tworzenie kopii zapasowych) przez agenta dla Hyper-V i agenta dla VMware (Windows).

  Skanowanie antywirusowe nie jest obsługiwane w przypadku kopii zapasowych utworzonych przez urządzenia wirtualne, takie jak agent dla VMware (urządzenie wirtualne), agent dla Virtuozzo czy agent dla Scale Computing HC3.
- Skanowane są tylko woluminy z systemem plików NTFS oraz partycjonowaniem GPT lub MBR.
- Jedyną obsługiwaną lokalizacją kopii zapasowych jest domyślna chmura. Magazyny lokalne i chmury należące do partnerów nie są obsługiwane.

© Acronis International GmbH, 2003-2024

- Wybierając kopie zapasowe do przeskanowania, można wybrać zestawy kopii zapasowych zawierające kopie zapasowe tworzone w ramach ciągłej ochrony danych (CDP). Zostaną jednak przeskanowane tylko te kopie zapasowe z zestawów, które nie są kopiami CDP. Dodatkowe informacje na temat kopii zapasowych CDP można znaleźć w sekcji "Ciągła ochrona danych" (s. 437).
- Przeprowadzając bezpieczne odzyskiwanie całego komputera, można wybrać zestaw kopii zapasowych obejmujący kopię CDP. Jednak w ramach tej operacji odzyskiwania nie zostaną wykorzystane dane z kopii zapasowej CDP. Aby odzyskać dane CDP, uruchom dodatkową operację odzyskiwania przy użyciu opcji **Pliki/foldery**.

© Acronis International GmbH, 2003-2024

Korzystanie z funkcji ochrony zaawansowanej

Domyślnie rozwiązanie Cyber Protect obejmuje funkcje dotyczące większości zagrożeń bezpieczeństwa cybernetycznego. Z funkcji można korzystać bez dodatkowych opłat. Można też włączyć funkcje zaawansowane w celu wzmocnienia ochrony obciążeń.

- Jeśli funkcja Ochrona zaawansowana jest dostępna dla użytkownika, będzie oznaczona w planie ochrony ikoną Funkcja zaawansowana .
- Jeśli funkcja Ochrona zaawansowana nie jest dla Ciebie dostępna, skontaktuj się z administratorem, aby włączyć wymagany pakiet ochrony zaawansowanej.
- Jeśli administrator umożliwił zakup dodatkowych pakietów zabezpieczeń, możesz się zdecydować na włączenie funkcji zaawansowanych. Zostanie wyświetlony komunikat z informacją o naliczaniu dodatkowych opłat.

Uwaga
Jeśli zostanie włączona choć jedna funkcja, trzeba będzie kupić odpowiedni pakiet ochrony zaawansowanej.

Uwaga
Jeśli wszystkie funkcje zaawansowane zostaną wyłączone w planie ochrony, odpowiedni pakiet ochrony zaawansowanej zostanie wyłączony.

Pakiet ochrony zaawansowanej	Funkcje ochrony zaawansowanej
Zaawansowane tworzenie kopii zapasowych	Chroni Twoje maszyny w sposób ciągły i gwarantuje, że nie zostaną utracone nawet te zmiany, które zostały wprowadzone w Twojej pracy w ostatniej chwili. Dostępne są między innymi następujące funkcje: • Odzyskiwanie jednym kliknięciem • Ciągła ochrona danych • Obsługa kopii zapasowych w przypadku klastrów programu Microsoft SQL Server i Microsoft Exchange – zawsze włączone grupy dostępności (AAG) i grupy dostępności bazy danych (DAG) • Obsługa kopii zapasowych oprogramowania MariaDB, MySQL, Oracle DB i SAP HANA • Mapa ochrony danych i raporty o zgodności z wymogami • Przetwarzanie danych poza hostem • Częstotliwość tworzenia kopii zapasowych w przypadku obciążeń Microsoft 365 i Google Workspace • Operacje zdalne dotyczące nośnika startowego • Bezpośrednie tworzenie kopii zapasowych w chmurze publicznej Microsoft Azure, Amazon S3 lub Wasabi
Zabezpieczenia	Chroni Twoje maszyny w sposób ciągły przed wszystkimi zagrożeniami związanymi

© Acronis International GmbH, 2003-2024

zaawansowane + Zaawansowana ochrona EDR	ze złośliwym oprogramowaniem. Dostępne są między innymi następujące funkcje: • Zarządzanie incydentami na scentralizowanej stronie incydentów • Wizualizowanie zakresu i wpływu incydentów • Zalecenia i kroki naprawcze • Sprawdzanie pod kątem ujawnionych publicznie ataków na używane obciążenia za pomocą kanałów dotyczących zagrożeń • Przechowywanie zdarzeń zabezpieczeń przez 180 dni • Ochrona przed wirusami i złośliwym oprogramowaniem z lokalnym wykrywaniem plików opartym na sygnaturach (z ochroną w czasie rzeczywistym) • Ochrona przed exploitami • Filtrowanie adresów URL • Zarządzanie zaporą w punktach końcowych • Kopie zapasowe na potrzeby analizy śledczej, skanowanie kopii zapasowych pod kątem złośliwego oprogramowania, bezpieczne odzyskiwanie, firmowa lista dozwolonych • Inteligentne plany ochrony (integracja z alertami CPOC) • Scentralizowane skanowanie kopii zapasowych pod kątem złośliwego oprogramowania • Wymazywanie zdalne • Moduł Microsoft Defender Antivirus • Microsoft Security Essentials
Zarządzanie zaawansowane	Umożliwia stosowanie poprawek do luk w zabezpieczeniach chronionych maszyn. Dostępne są między innymi następujące funkcje: • Zarządzanie poprawkami • Kondycje dysków • Inwentaryzacja oprogramowania • Bezpieczne wdrażanie poprawek • Skrypty cybernetyczne • Pomoc zdalna • Przesyłanie i udostępnianie plików • Wybieranie sesji do połączenia • Obserwowanie obciążeń w multiwidoku • Tryby połączeń: Sterowanie, Tylko do przeglądania i Zasłona • Połączenie przez aplikację Quick Assist • Protokoły połączeń zdalnych: NEAR i Udostępnianie ekranu firmy Apple • Nagrywanie sesji w przypadku połączeń NEAR • Przesyłanie zrzutu ekranu • Raport z historii sesji • 24 monitory • Monitorowanie typu Wykrywanie progów • Monitorowanie typu Wykrywanie anomalii

© Acronis International GmbH, 2003-2024

Advanced Data Loss Prevention	Zapobiega wyciekom informacji wrażliwych z chronionych maszyn. Dostępne są między innymi następujące funkcje: • Zapobieganie utracie danych z obciążeń uwzględniające zawartość obsługiwane za pośrednictwem urządzeń peryferyjnych i komunikacji sieciowej • Wbudowane automatyczne wykrywanie danych osobowych (personally identifiable information, PII), chronionych informacji dotyczących zdrowia (protected health information, PHI) oraz danych zgodnych z normą bezpieczeństwa danych w branży kart płatniczych (Payment Card Industry Data Security Standard, PCI DSS), a także dokumentów z kategorii „Oznaczono jako poufne” • Automatyczne tworzenie zasad zapobiegania utracie danych z opcjonalną pomocą dla użytkownika • Adaptacyjne wdrażanie zapobiegania utracie danych z automatycznym korygowaniem zasad dzięki uczeniu się • Centralne, oparte na chmurze tworzenie dzienników inspekcji, generowanie alertów i powiadamianie użytkowników

Advanced Data Loss Prevention

Moduł Advanced Data Loss Prevention analizuje zawartość i kontekst przesyłania danych na chronionych obciążeniach i na podstawie zasad przepływów danych zapobiega wyciekowi poufnych danych za pośrednictwem urządzeń peryferyjnych lub operacji przesyłania w ramach sieci firmowej bądź poza nią.

Funkcje modułu Advanced Data Loss Prevention można dodać do dowolnego planu ochrony w ramach dzierżawcy-klienta, jeśli dla tego klienta włączono usługę Ochrona i pakiet Advanced Data Loss Prevention.

Zanim zaczniesz korzystać z modułu Advanced Data Loss Prevention, koniecznie zapoznaj się z podstawowymi pojęciami oraz logiką zarządzania tym modułem, które opisano w podręczniku Podstawowe informacje.

Warto też zapoznać się z dokumentem Dane techniczne.

Tworzenie zasad i reguł przepływów danych

Kluczowa zasada zapobiegania utracie danych wymaga, aby użytkownicy korporacyjnego systemu informatycznego mogli korzystać z poufnych danych tylko w zakresie niezbędnym do wykonywania swoich obowiązków służbowych. Wszelkie inne operacje przesyłania poufnych danych — nieistotne z perspektywy procesów biznesowych — powinny być blokowane. Dlatego kluczowe znaczenie ma rozróżnienie między operacjami przesyłania lub przepływami danych związanymi z działalnością biznesową a operacjami bezzasadnymi.

Zasady przepływów danych obejmują reguły określające, które przepływy danych są dozwolone, a które zabronione, zapobiegając w ten sposób nieuprawnionemu przekazywaniu informacji

© Acronis International GmbH, 2003-2024

wrażliwych, gdy moduł Zapobieganie utracie danych jest włączony w planie ochrony i działa w trybie egzekwowania.

Każda kategoria poufności w zasadach zawiera jedną regułę domyślną, oznaczoną gwiazdką (*), oraz co najmniej jedną wyraźniejszą regułę (niedomyślną), która określa przepływy danych dla konkretnych użytkowników lub grup. Dodatkowe informacje na temat typów reguł można znaleźć w podręczniku Podstawowe informacje.

Zasady przepływów danych są zwykle tworzone automatycznie, gdy moduł Advanced Data Loss Prevention działa w trybie obserwacji. Na zbudowanie reprezentatywnych zasad przepływów danych potrzeba około miesiąca, ale czas ten może być inny — w zależności od procesów biznesowych danej organizacji. Zasady przepływów danych mogą też być tworzone, konfigurowane i edytowane ręcznie przez administratora firmy bądź jednostki.

Aby aktywować automatyczne tworzenie zasad przepływów danych,

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
3. Kliknij **Utwórz plan**.
4. Rozwiń sekcję **Zapobieganie utracie danych** i kliknij wiersz **Tryb**.
5. W oknie dialogowym Tryb wybierz **Tryb obserwacji** i wskaż, jak mają być traktowane operacje przesyłania danych:

Opcja	Opis
Zezwalaj w przypadku wszystkich	Wszystkie operacje przesyłania poufnych danych z obciążeń użytkowników są traktowane jako niezbędne z perspektywy procesu biznesowego i bezpieczne. W przypadku każdego wykrytego przepływu danych, który nie jest zgodny z już zdefiniowaną regułą, jest tworzona nowa reguła.
Uzasadnij wszystkie	Wszystkie operacje przesyłania poufnych danych z obciążeń użytkowników są traktowane jako niezbędne z perspektywy procesu biznesowego, ale ryzykowne. Dlatego w przypadku każdej przechwyconej operacji przesyłania poufnych danych do dowolnego odbiorcy lub miejsca docelowego — zarówno w ramach organizacji, jak i poza nią — która nie jest zgodna z wcześniej utworzoną regułą przepływów danych, użytkownik musi podać jednorazowe uzasadnienie biznesowe. Po przekazaniu uzasadnienia w zasadach przepływów danych jest tworzona nowa reguła przepływu danych.
Mieszana	Logika Zezwalaj w przypadku wszystkich jest stosowana do wszystkich wewnętrznych przepływów poufnych danych, a logika Uzasadnij wszystkie — do wszystkich przepływów zewnętrznych. **Uwaga** Dodatkowe informacje na temat danych wewnętrznych i zewnętrznych można znaleźć w artykule Automatyczne wykrywanie miejsca docelowego.

© Acronis International GmbH, 2003-2024

6. Zapisz plan ochrony i zastosuj go do obciążeń, z których chcesz zbierać dane w celu opracowywania zasad.

Uwaga
W trybie obserwacji nie można zapobiec wyciekowi danych.

Aby ręcznie skonfigurować zasady przepływów danych,

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona** > **Zasady przepływów danych**.
2. Kliknij **Nowa reguła przepływu danych**.
   Po prawej stronie zostanie wyświetlone okienko Nowa reguła przepływu danych.
3. Wybierz kategorię poufności, dodaj nadawcę i odbiorcę, a następnie określ uprawnienia do przesyłania danych dla wybranej kategorii, nadawcy i odbiorcy.

Opcja	Opis
Pozwól	Zezwól nadawcy na przesyłanie danych z tej kategorii poufności do wybranego odbiorcy.
Wyjątek	Nie zezwalaj nadawcy na przesyłanie danych z tej kategorii poufności do wybranego odbiorcy, ale zezwól nadawcy na zgłoszenie wyjątku od reguły w przypadku konkretnej operacji przesyłania danych. Gdy nadawca spróbuje przesłać dane z tej kategorii poufności do wybranego odbiorcy, zablokuj operację przesyłania i poproś nadawcę o zgłoszenie wyjątku, aby mógł uzyskać zezwolenie na daną operację przesyłania danych. Po zgłoszeniu wyjątku będzie można kontynuować przesyłanie danych. **Ważne** W ciągu 5 minut od zgłoszenia wyjątku będą dozwolone też kolejne operacje przesyłania danych z tej kategorii poufności między danym nadawcą a odbiorcą.
Odmów	Nie zezwalaj nadawcy na przesyłanie danych z tej kategorii poufności do wybranego odbiorcy i nie zezwalaj nadawcy na proszenie o wyjątek od reguły.

4. (Opcjonalnie) Wybierz czynność, która ma zostać wykonana po wyzwoleniu reguły.

Czynność	Opis
Zapisz w dzienniku	W przypadku wyzwolenia reguły w dzienniku inspekcji zostanie zapisany rekord zdarzenia. Zalecamy wybranie tej czynności w przypadku reguły z uprawnieniem **Wyjątek**.
Wygeneruj alert	Gdy reguła zostanie wyzwolona, wygeneruj alert na karcie Cyber Protect **Alerty**. Jeśli włączono powiadomienia dla administratora, zostanie też wysłane powiadomienie e-mail.
Powiadom użytkownika w razie odmowy przesyłania danych	Ta opcja umożliwia włączenie powiadamiania użytkownika w czasie rzeczywistym za pomocą ostrzeżenia wyświetlanego na ekranie w przypadku wyzwolenia reguły.

5. Kliknij **Zapisz**.

© Acronis International GmbH, 2003-2024

6. Powtórz kroki 2–5, aby utworzyć wiele reguł o różnych kategoriach poufności i opcjach, a następnie sprawdź, czy nowo utworzone reguły odpowiadają wybranym opcjom.

Struktura zasad przepływów danych

W widoku **Zasady przepływów danych** reguły są pogrupowane według kontrolowanych przez nie kategorii poufnych danych. Bezpośrednio nad grupą reguł jest wyświetlany identyfikator kategorii poufności.

- Wrażliwe
  - Chronione informacje dotyczące zdrowia (PHI)
  - Dane osobowe (PII)
  - Norma bezpieczeństwa danych w branży kart płatniczych (PCI DSS)
  - Oznaczono jako poufne
- Niewrażliwe

Więcej informacji na temat koncepcji i funkcji zasad przepływów danych można znaleźć w podręczniku Podstawowe informacje.

Struktura reguł

Każda reguła obejmuje niżej wymienione elementy.

- **Kategoria poufności**
  - **Chronione informacje dotyczące zdrowia (PHI)**
  - **Dane osobowe (PII)**
  - **Norma bezpieczeństwa danych w branży kart płatniczych (PCI DSS)**
  - **Oznaczono jako poufne**

    Zobacz "Definicje poufnych danych" (s. 943)
- **Nadawca** — oznacza inicjatora operacji przesyłania danych kontrolowanej przez daną regułę. Może to być jeden użytkownik albo lista bądź grupa użytkowników.
  - **Dowolne wewnętrzne** — grupa użytkowników, do której należą wszyscy wewnętrzni użytkownicy z organizacji.
  - **Kontakt / Z organizacji** — konto systemu Windows organizacji rozpoznane przez usługę Advanced Data Loss Prevention, a także każde inne konto (w tym używane przez aplikacje do komunikacji pochodzące od innych firm), z których wcześniej korzystało dane konto systemu Windows.
  - **Kontakt / Tożsamość niestandardowa** — identyfikator użytkownika wewnętrznego podany w jednym z następujących formatów: adres e-mail, identyfikator Skype, identyfikator ICQ, identyfikator IRC, adres e-mail na platformie Jabber, adres e-mail w usłudze Mail.ru Agent, numer telefonu Viber, adres e-mail w usłudze Zoom.
    W celu określenia grupy kontaktów można użyć następujących symboli wieloznacznych:

© Acronis International GmbH, 2003-2024

        - ***** — zastępuje dowolną liczbę znaków
        - **?** — zastępuje jeden dowolny znak
- **Odbiorca** — oznacza obiekt docelowy operacji przesyłania danych kontrolowanej przez daną regułę. Może to być jeden użytkownik albo lista bądź grupa użytkowników, a także dowolny inny obiekt docelowy spośród wymienionych niżej.
    - **Dowolny** — dowolny typ odbiorcy obsługiwany przez usługę Advanced DLP.
    - **Kontakt / Dowolny kontakt** — dowolny kontakt wewnętrzny lub zewnętrzny.
    - **Kontakt / Dowolny kontakt wewnętrzny** — dowolny kontakt będący użytkownikiem wewnętrznym (zobacz "Automatyczne wykrywanie miejsca docelowego" (s. 942)).
    - **Kontakt / Dowolny kontakt zewnętrzny** — dowolny kontakt będący osobą spoza organizacji lub podmiotem zewnętrznym.
    - **Kontakt / Z organizacji** — ta sama zasada, która została opisana w przypadku pola Nadawca.
    - **Kontakt / Tożsamość niestandardowa** — ta sama zasada, która została opisana w przypadku pola Nadawca.
    - **Usługi udostępniania plików** — identyfikator kontrolowanej usługi udostępniania plików.
    - **Portal społecznościowy** — identyfikator kontrolowanego portalu społecznościowego.
    - **Host / Dowolny host** — każdy komputer rozpoznany przez usługę Advanced DLP jako wewnętrzny lub zewnętrzny.
    - **Host / Dowolny host wewnętrzny** — każdy komputer rozpoznany przez usługę Advanced DLP jako wewnętrzny.
    - **Host / Dowolny host zewnętrzny** — każdy komputer rozpoznany przez usługę Advanced DLP jako zewnętrzny.
    - **Host / Określony host** — identyfikator komputera podany jako nazwa hosta (np. nazwa FQDN) lub adres IP (IPv4 lub IPv6).
    - **Urządzenie / Dowolne urządzenie** — dowolne urządzenie peryferyjne połączone z obciążeniem.
    - **Urządzenie / Magazyn zewnętrzny** — magazyn wymienny lub przekierowany zamapowany dysk połączony z obciążeniem.
    - **Urządzenie / Zaszyfrowane urządzenie wymienne** — wymienne urządzenie pamięci masowej zaszyfrowane za pomocą funkcji BitLocker To Go.
    - **Urządzenie / Przekierowany schowek** — przekierowany schowek połączony z obciążeniem.
    - **Drukarki** — dowolna drukarka lokalna lub sieciowa połączona z obciążeniem.
- **Uprawnienie** — kontrola prewencyjna egzekwowana w stosunku do operacji przesyłania danych kontrolowanej przez daną regułę. Bardziej szczegółowy opis można znaleźć w sekcji Uprawnienia w regułach przepływów danych.
- **Czynność** — nieprewencyjna czynność wykonywana w przypadku wyzwolenia danej reguły. Domyślnie to pole ma ustawioną wartość „Brak czynności”. Dostępne są następujące opcje:
    - **Zapisz w dzienniku** — w przypadku wyzwolenia reguły w dzienniku inspekcji zostanie zapisany rekord zdarzenia.

© Acronis International GmbH, 2003-2024

- **Powiadom użytkownika w razie odmowy przesyłania danych** — użytkownik zostanie powiadomiony o uruchomieniu reguły w czasie rzeczywistym za pomocą ostrzeżenia wyświetlanego na ekranie.
- **Wygeneruj alert** — w przypadku wyzwolenia reguły administrator otrzyma alert.

Ostrzeżenie!
W przypadku wybrania opcji **Brak czynności** po wyzwoleniu reguły:

- do dziennika inspekcji nie jest dodawany żaden rekord zdarzenia;
- do administratora nie jest wysyłany żaden alert;
- na ekranie nie jest wyświetlane żadne powiadomienie dla użytkownika.

Co powoduje wyzwolenie reguły?

Operacja przesyłania danych jest zgodna z regułą przepływu danych, jeśli są spełnione wszystkie następujące warunki:

- Wszyscy nadawcy przesyłanych danych znajdują się na liście lub należą do grupy użytkowników określonej w polu **Nadawca** reguły.
- Wszyscy odbiorcy przesyłanych danych znajdują się na liście lub należą do grupy użytkowników określonej w polu **Odbiorca** reguły.
- Przesyłane dane są zgodne z wartością **Kategoria poufności** reguły.

Dostosowywanie uprawnień w regułach przepływów danych

Moduł Advanced Data Loss Prevention obsługuje trzy rodzaje uprawnień w regułach przepływów danych. Uprawnienia można konfigurować w przypadku każdej reguły z osobna.

Pozwól (przyzwolenie)	Operacje przesyłania danych, które pasują do zdefiniowanej w regule kombinacji kategorii poufności, nadawcy i odbiorcy, są dozwolone.
Wyjątek (zakaz)	Operacje przesyłania danych, które pasują do zdefiniowanej w regule kombinacji kategorii poufności, nadawcy i odbiorcy, są zabronione, ale nadawca może zgłosić wyjątek od reguły, aby uzyskać pozwolenie na określoną operację przesyłania. **Ważne** W ciągu 5 minut od zgłoszenia wyjątku będą dozwolone też kolejne operacje przesyłania danych z tej kategorii poufności między danym nadawcą a odbiorcą.
Odmów (zakaz)	Operacje przesyłania danych, które pasują do zdefiniowanej w regule kombinacji kategorii poufności, nadawcy i odbiorcy, są zabronione i nadawca nie może zgłosić wyjątku.

Ponadto do uprawnień **Pozwól** i **Wyjątek** można przypisywać flagi priorytetu, aby zwiększyć elastyczność zarządzania zasadami. Za pomocą tego ustawienia można zastąpić uprawnienia ustawione dla określonych grup w innych regułach przepływów danych. Można ich użyć w celu

© Acronis International GmbH, 2003-2024

zastosowania reguły przepływu danych grupy tylko w przypadku niektórych jej członków. Aby to osiągnąć, trzeba utworzyć regułę przepływów danych dla określonych użytkowników, których chce się wykluczyć z reguł grupy, a następnie nadać ich uprawnieniom priorytet w stosunku do ograniczeń przepływów danych skonfigurowanych w regułach dla grupy, do której należą ci użytkownicy. Informacje na temat priorytetów uprawnień w przypadku łączenia reguł można znaleźć w sekcji "Łączenie reguł przepływów danych" (s. 934).

Ważne
Przed przełączeniem zasad firmy lub jednostki z trybu obserwacji w tryb egzekwowania zdecydowanie należy zmienić domyślne reguły dla każdej kategorii poufnych danych ze stanu przyzwolenia na zakaz. Reguły domyślne są w widoku **Zasady przepływów danych** oznaczone gwiazdką (*). Dodatkowe informacje na temat typów reguł można znaleźć w podręczniku Podstawowe informacje.

Aby edytować uprawnienia w regułach

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Ochrona** > **Zasady przepływów danych**.
3. Wybierz regułę, którą chcesz edytować, i kliknij **Edytuj** nad listą reguł.
   Zostanie otwarte okno **Edytuj regułę przepływu danych**.
4. W sekcji **Uprawnienie** wybierz **Pozwól**, **Wyjątek** lub **Odmów**.
5. (Opcjonalnie) Aby nadać priorytet uprawnieniu **Pozwól** lub **Wyjątek** tej reguły nad uprawnieniami w innych regułach, zaznacz pole wyboru **Nadaj priorytet**.
   Nie należy używać tego pola wyboru do określania priorytetu reguły przepływu danych w stosunku do domyślnej reguły Dowolne > Inna reguła, ponieważ w zasadach domyślnie ma ona zawsze najniższy priorytet.
   Informacje na temat priorytetów uprawnień w przypadku łączenia reguł można znaleźć w sekcji "Łączenie reguł przepływów danych" (s. 934).
6. (Opcjonalnie) Wybierz czynność, która ma zostać wykonana po wyzwoleniu reguły.
7. Zapisz zmiany w regule.

Łączenie reguł przepływów danych

Jeśli operacja przesyłania danych jest zgodna z więcej niż jedną regułą, uprawnienia oraz czynności skonfigurowane dla wszystkich reguł są łączone i stosowane w niżej opisany sposób.

Uprawnienia

Jeśli operacja przesyłania danych jest zgodna z więcej niż jedną regułą i reguły te mają różne uprawnienia w przypadku tej samej kategorii danych, regułą nadrzędną jest ta, której uprawnienia mają wyższy priorytet według następującej listy priorytetów uprawnień (w kolejności malejącej):

1. Wyjątek z flagą **Priorytetowe**
2. Pozwól z flagą **Priorytetowe**

© Acronis International GmbH, 2003-2024

3. Odmów
4. Wyjątek
5. Pozwól

Jeśli operacja przesyłania danych jest zgodna z więcej niż jedną regułą i reguły te mają różne uprawnienia w przypadku różnych kategorii danych, reguła nadrzędna jest ustalana według następującej logiki:

1. Najbardziej restrykcyjne uprawnienia reguł są definiowane w przypadku każdej kategorii poufności, do której pasuje dana operacja przesyłania danych.
2. Egzekwowane są najbardziej restrykcyjne uprawnienia z określonych w punkcie 1.

Przykład

Operacja przesyłania pliku jest zgodna z trzema regułami w różnych kategoriach poufności, jak opisano poniżej:

Kategoria poufności	Uprawnienie
Dane osobowe	Pozwól — Priorytetowe
PHI	Wyjątek — Priorytetowe
PCI	Odmów

Zostanie zastosowane uprawnienie Odmów.

Czynności

Jeśli operacja przesyłania danych jest zgodna z więcej niż jedną regułą i reguły te mają skonfigurowane różne opcje w polu **Czynność**, wykonywane są wszystkie czynności skonfigurowane we wszystkich wyzwolonych regułach.

Przegląd zasad i zarządzanie nimi

Zanim automatycznie utworzone podstawowe zasady przepływów danych zaczną być egzekwowane, trzeba je przejrzeć i zweryfikować oraz muszą zostać zatwierdzone przez klienta, ponieważ to właśnie on z natury rzeczy zna wszystkie szczegóły swoich procesów biznesowych i może ocenić, czy są one spójnie interpretowane w podstawowych zasadach. Ponadto klient może wskazać braki, które są następnie usuwane przez administratora partnera.

Podczas przeglądu zasad administrator partnera przedstawia podstawowe zasady przepływów danych klientowi, który dokonuje przeglądu każdego przepływu danych w zasadach i weryfikuje ich zgodność z rzeczywistymi procesami biznesowymi. Sprawdzanie poprawności nie wymaga żadnych umiejętności technicznych, ponieważ reguły są intuicyjnie przejrzyście przedstawione w konsoli Cyber Protect: w każdej z nich jest opisane, kto jest nadawcą i odbiorcą przepływu wrażliwych danych.

© Acronis International GmbH, 2003-2024

Na podstawie instrukcji klienta administrator partnera ręcznie koryguje podstawowe zasady, edytując, usuwając i tworząc reguły przepływów danych. Po zatwierdzeniu przez klienta przejrzane zasady są egzekwowane na chronionych obciążeniach przez przełączenie zastosowanego do nich planu ochrony w tryb egzekwowania.

Ważną rzeczą jest, by przed rozpoczęciem egzekwowania przejrzanych zasad zmienić uprawnienie **Pozwól** we wszystkich automatycznie utworzonych regułach domyślnych dla kategorii poufnych danych na **Odmów** lub **Wyjątek**. Uprawnienie **Odmów** nie może zostać zastąpione przez użytkowników, a uprawnienie **Wyjątek** blokuje operacje przesyłania zgodne z regułą, ale umożliwia użytkownikom uchylenie blokady w sytuacjach awaryjnych przez zgłoszenie wyjątku związanego z celami biznesowymi.

Odnawianie zasad przepływów danych

Gdy proces biznesowy firmy lub jej jednostki ulega znacznej zmianie, trzeba odnowić zasady zapobiegania utracie danych w celu ich dostosowania do zmian w zakresie przepływów poufnych danych w zaktualizowanym procesie biznesowym. Odnowienie zasad jest też konieczne w przypadku zmiany roli zawodowej pracownika — należy wówczas odnowić również tę część zasad jednostki, która ma na celu ochronę obciążenia pracownika.

Przepływ pracy związany z zarządzaniem zasadami usługi Advanced DLP umożliwia administratorom zautomatyzowanie odnawiania zasad dla całej firmy, jednostki, użytkownika lub części użytkowników w jednostce.

Odnawianie zasad dla firmy lub jednostki

Wszystkich opcji trybu obserwacji można używać do odnawiania wszystkich zasad firmy lub jednostki, a także części zasad jednostki dla wybranych użytkowników w jednostce.

Aby odnowić zasady dla firmy lub jednostki

Proces odnawiania obejmuje następujące kroki, które muszą zostać wykonane przez administratora firmy lub partnera zarządzającego jej obciążeniami.

1. Usuń wszystkie niedomyślne reguły z egzekwowanych zasad.
2. Aby rozpocząć odnawianie, zmień plan ochrony z usługą Advanced DLP zastosowaną do firmy lub jednostki na jedną z opcji trybu obserwacji, w zależności od tego, która z nich jest optymalna w przypadku danej firmy lub jednostki, a następnie zastosuj plan do wszystkich obciążeń firmy lub jednostki.
3. Po zakończeniu okresu odnawiania przeanalizuj wraz z klientem nowe zasady firmy lub jednostki, w razie potrzeby wprowadź poprawki i uzyskaj zatwierdzenie ze strony klienta.
4. Zmień plan ochrony zastosowany do obciążeń firmy lub jednostki na odpowiednią opcję trybu egzekwowania, którą klient uzna za optymalną z perspektywy zapobiegania wyciekom danych z obciążeń jednostki.

© Acronis International GmbH, 2003-2024

Odnawianie zasad dla wybranych użytkowników z firmy lub jednostki

Zasady na poziomie użytkownika można odnowić przy użyciu dowolnej opcji trybu obserwacji oraz trybu egzekwowania adaptacyjnego.

Odnawianie zasad użytkownika przy użyciu trybu obserwacji

Użycie trybu obserwacji w celu odnowienia zasad dla użytkownika lub części użytkowników w firmie (bądź jednostce) ma następujące cechy szczególne: zasady przepływów danych egzekwowane dla całej firmy (lub jednostki) nie są egzekwowane w przypadku operacji przesyłania danych użytkownika w okresie odnawiania. W związku z tym podczas odnawiania można utworzyć nowe indywidualne reguły dla użytkownika, które mogą być sprzeczne lub zgodne z istniejącymi regułami grupy w zasadach egzekwowanych w przypadku firmy (lub jednostki). Po zakończeniu odnawiania i wznowieniu egzekwowania zasad w przypadku operacji przesyłania danych użytkownika to, czy te nowe indywidualne reguły utworzone dla użytkownika faktycznie zostaną zastosowane do jego operacji przesyłania danych, zależy od ich priorytetów w porównaniu z innymi regułami, z którymi te operacje przesyłania danych są zgodne.

Aby odnowić zasady dla użytkownika w ramach trybu obserwacji

Proces odnawiania obejmuje następujące kroki, które muszą zostać wykonane przez administratora firmy lub partnera zarządzającego jej obciążeniami.

1. Usuń z zasad egzekwowanych w przypadku firmy (lub jednostki) wszystkie niedomyślne reguły, w których dany użytkownik jest jedynym nadawcą.
2. Usuń użytkownika z list nadawców wszystkich niedomyślnych reguł przepływów danych w ramach egzekwowanych zasad.
3. Utwórz nowy plan ochrony z usługą Advanced DLP w trybie obserwacji i zastosuj go do obciążenia użytkownika, aby rozpocząć okres odnawiania (obserwacji).
   Czas trwania okresu odnawiania zależy od tego, jak długo użytkownik może wykonywać wszystkie lub 90–95% swoich standardowych czynności służbowych, które wiążą się z przesyłaniem poufnych danych z jego obciążeń.
4. Po zakończeniu okresu odnawiania przeanalizuj nowe reguły dotyczące tego użytkownika, które dodano do egzekwowanych zasad, w razie potrzeby wprowadź w nich poprawki i uzyskaj zatwierdzenie ze strony klienta.
5. Przełącz plan ochrony zastosowany do obciążenia użytkownika w tryb **Ścisłe egzekwowanie** lub **Egzekwowanie adaptacyjne** — w zależności od tego, którą opcję klient uzna za optymalną z perspektywy zapobiegania wyciekom danych z obciążenia użytkownika.
   Można też ponownie zastosować do obciążenia użytkownika plan ochrony zastosowany w przypadku firmy (lub jednostki).

Odnawianie zasad użytkownika przy użyciu trybu Egzekwowanie adaptacyjne

Odnowienie zasad dla wybranego użytkownika bądź części wszystkich użytkowników w firmie (lub jednostce) można przeprowadzić za pomocą trybu egzekwowania adaptacyjnego planu ochrony z usługą Advanced DLP zastosowanego do obciążenia użytkownika.

© Acronis International GmbH, 2003-2024

Uwaga
Ta metoda odnawiania zasad ma następujące cechy szczególne: egzekwowane reguł firmy (jednostki) w przypadku grup nadawców, do których należy użytkownik (np. Dowolne wewnętrzne) są egzekwowane również w przypadku operacji przesyłania danych od tego użytkownika podczas odnawiania. W związku z tym odnowienie nie spowoduje utworzenia nowych reguł indywidualnych dla użytkownika, które mogłyby być sprzeczne lub zgodne z już istniejącymi regułami dla grup nadawców. Która z tych dwóch metod jest bardziej efektywna w przypadku odnawiania zasad dla użytkowników w kontekście danego klienta zależy od jego konkretnych wymagań w zakresie bezpieczeństwa środowiska IT.

Aby odnowić zasady dla użytkownika w ramach trybu egzekwowania adaptacyjnego

Proces odnawiania obejmuje następujące kroki, które muszą zostać wykonane przez administratora firmy lub partnera zarządzającego jej obciążeniami.

1. Usuń z zasad egzekwowanych w przypadku firmy (jednostki) wszystkie niedomyślne reguły, w których dany użytkownik jest jedynym nadawcą.
2. Usuń użytkownika z list nadawców wszystkich niedomyślnych reguł przepływów danych w ramach egzekwowanych zasad.
3. W przypadku wszystkich reguł domyślnych w zasadach egzekwowanych wobec firmy (lub jednostki) ustaw uprawnienia na **Wyjątek** i w polu **Czynność** wybierz **Zapisz w dzienniku**.
4. Jeśli plan ochrony obecnie zastosowany do obciążenia użytkownika ma ustawiony tryb **Ścisłe egzekwowanie**, utwórz nowy plan ochrony z usługą Advanced DLP i zastosuj go do obciążenia użytkownika w trybie **Egzekwowanie adaptacyjne**, aby rozpocząć okres odnawiania.
   Czas trwania okresu odnawiania zależy od tego, jak długo użytkownik może wykonywać wszystkie lub 90–95% swoich standardowych czynności służbowych, które wiążą się z przesyłaniem poufnych danych z jego obciążeń.
5. Po zakończeniu okresu odnawiania przeanalizuj nowe reguły dotyczące tego użytkownika, które dodano do egzekwowanych zasad, w razie potrzeby wprowadź w nich poprawki i uzyskaj zatwierdzenie ze strony klienta.
6. Przełącz plan ochrony zastosowany do obciążenia użytkownika w tryb **Ścisłe egzekwowanie** lub pozostaw go w trybie **Egzekwowanie adaptacyjne** — w zależności od tego, którą opcję klient uzna za optymalną z perspektywy zapobiegania wyciekom danych z obciążenia użytkownika. Można też ponownie zastosować do obciążenia użytkownika plan ochrony zastosowany w przypadku firmy (lub jednostki).

Włączanie modułu Advanced Data Loss Prevention w planach ochrony

Funkcje modułu Advanced Data Loss Prevention można dodać do dowolnego planu ochrony w ramach dzierżawcy-klienta, jeśli dla tego klienta włączono usługę Ochrona i pakiet Advanced Data Loss Prevention.

© Acronis International GmbH, 2003-2024

Advanced DLP to zaawansowany moduł grupy funkcji zapobiegających utracie danych. Funkcje Advanced DLP i Kontrola urządzeń mogą być używane niezależnie lub razem (w jednym planie ochrony lub w dwóch planach chroniących to samo obciążenie). Jeśli są używane razem, ich funkcjonalne możliwości są koordynowane w następujący sposób.

- Kontrola urządzeń przestaje kontrolować dostęp użytkownika do tych lokalnych kanałów, w których Advanced DLP sprawdza zawartość przesyłanych danych. Jednak funkcja Kontrola urządzeń zachowuje kontrolę nad następującymi typami urządzeń, jeśli są one skonfigurowane jako Tylko do odczytu lub Odmowa dostępu:
  - Wymienny
  - Zaszyfrowane urządzenie wymienne
  - Zamapowany dysk

  Jeśli na przykład masz włączoną zarówno funkcję Kontrola urządzeń, jak i Advanced DLP w jednym planie ochrony lub w dwóch planach chroniących to samo obciążenie, a w funkcji Kontrola urządzeń masz skonfigurowany dostęp tylko do odczytu w przypadku urządzeń USB, dostęp tylko do odczytu zostanie zastosowany do wszystkich urządzeń USB, z wyjątkiem tych uwzględnionych na liście dozwolonych, niezależnie od ustawień dostępu w module Advanced DLP. Jeśli w funkcji Kontrola urządzeń domyślnie jest skonfigurowana opcja Włącz dostęp, zostanie zastosowane ustawienie dostępu określone w module Advanced DLP.
- Dostęp użytkowników do następujących kanałów lokalnych i urządzeń peryferyjnych z listy dozwolonych jest egzekwowany przez funkcję Kontrola urządzeń:
  - Dyski optyczne
  - Dyskietki
  - Urządzenia mobilne połączone przy użyciu protokołu MTP
  - Adaptery Bluetooth
  - Schowek systemu Windows
  - Zarejestrowane zrzuty ekranu
  - Urządzenia USB i typy urządzeń (z wyjątkiem magazynów wymiennych i szyfrowanych)

Aby utworzyć plan ochrony przy użyciu modułu Advanced DLP

1. Przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Kliknij **Utwórz plan**.
3. Rozwiń sekcję **Zapobieganie utracie danych** i kliknij wiersz **Tryb**.
   Zostanie otwarte okno dialogowe **Tryb**.
   - Aby rozpocząć tworzenie lub odnawianie zasad przepływów danych, wybierz **Tryb obserwacji** i wskaż, jak mają być traktowane operacje przesyłania danych:

Opcja	Opis
Zezwalaj w przypadku	Wszystkie operacje przesyłania poufnych danych z obciążeń użytkowników są traktowane jako niezbędne z perspektywy procesu biznesowego i bezpieczne. W

© Acronis International GmbH, 2003-2024

Opcja	Opis
wszystkich	przypadku każdego wykrytego przepływu danych, który nie jest zgodny z już zdefiniowaną regułą, jest tworzona nowa reguła.
Uzasadnij wszystkie	Wszystkie operacje przesyłania poufnych danych z obciążeń użytkowników są traktowane jako niezbędne z perspektywy procesu biznesowego, ale ryzykowne. Dlatego w przypadku każdej przechwyconej operacji przesyłania poufnych danych do dowolnego odbiorcy lub miejsca docelowego — zarówno w ramach organizacji, jak i poza nią — która nie jest zgodna z wcześniej utworzoną regułą przepływów danych, użytkownik musi podać jednorazowe uzasadnienie biznesowe. Po przekazaniu uzasadnienia w zasadach przepływów danych jest tworzona nowa reguła przepływu danych.
Mieszana	Logika Zezwalaj w przypadku wszystkich jest stosowana do wszystkich wewnętrznych operacji przesyłania poufnych danych, a logika Uzasadnij wszystkie — do wszystkich zewnętrznych przepływów zewnętrznych operacji przesyłania poufnych danych. Definicję wewnętrznych miejsc docelowych można znaleźć w sekcji "Automatyczne wykrywanie miejsca docelowego" (s. 942)

Ostrzeżenie!

- Wybierz **Tryb obserwacji** tylko w sytuacji, gdy jeszcze nie zostały utworzone zasady przepływów danych lub gdy odnawiasz zasady. Zanim zaczniesz odnawianie zasad, zobacz "Odnawianie zasad przepływów danych" (s. 936).
- W trybie obserwacji nie można zapobiec wyciekowi danych. Zobacz Tryb obserwacji w podręczniku Podstawowe informacje.

- Aby egzekwować już istniejące zasady przepływów danych, wybierz **Tryb egzekwowania**, a następnie wybierz, jak ściśle mają być egzekwowane zasady przepływów danych:

Opcja	Opis
Ścisłe egzekwowanie	Zasady przepływów danych są egzekwowane w ich obecnym stanie i nie są rozszerzane o nowe przyzwalające reguły w przypadku wykrycia wcześniej nieobserwowanych przepływów poufnych danych. Zobacz Ścisłe egzekwowanie w podręczniku Podstawowe informacje.
Egzekwowanie adaptacyjne (egzekwowanie z nauką)	Egzekwowane zasady nadal automatycznie się dostosowują do tych operacji biznesowych, które nie zostały wykonane w czasie obserwacji, lub do zmian w procesach biznesowych. Tryb ten umożliwia rozszerzenie egzekwowanych zasad przepływów danych na podstawie nowo wyuczonych przepływów danych wykrytych na obciążeniach. Zobacz Egzekwowanie adaptacyjne w podręczniku Podstawowe informacje.

© Acronis International GmbH, 2003-2024

Ważne
Przed przełączeniem zasad firmy lub jednostki z trybu obserwacji w tryb egzekwowania zdecydowanie należy zmienić domyślne reguły dla każdej kategorii poufnych danych ze stanu przyzwolenia na zakaz. Reguły domyślne są w widoku **Zasady przepływów danych** oznaczone gwiazdką (*). Dodatkowe informacje na temat typów reguł można znaleźć w podręczniku Podstawowe informacje.

4. Kliknij **Gotowe**, aby zamknąć okno dialogowe Tryb.
5. (Opcjonalnie) Aby skonfigurować optyczne rozpoznawanie znaków, listy dozwolonych i inne opcje ochrony, kliknij **Ustawienia zaawansowane**.
   Informacje na temat dostępnych opcji można znaleźć w sekcji "Ustawienia zaawansowane" (s. 941).
6. Zapisz plan ochrony i zastosuj go do obciążeń, które chcesz chronić.

Ustawienia zaawansowane

Ustawienia zaawansowane w planach ochrony z włączoną usługą Advanced Data Loss Prevention umożliwiają podniesienie jakości inspekcji zawartości danych w kanałach kontrolowanych przez usługę Advanced Data Loss Prevention, a także wyłączenie z prewencyjnych kontroli operacji przesyłania danych do typów urządzeń peryferyjnych z listy dozwolonych, kategorii komunikacji sieciowej i hostów docelowych oraz operacji przesyłania danych inicjowanych przez aplikacje z listy dozwolonych. Można skonfigurować następujące ustawienia zaawansowane:

- **Optyczne rozpoznawanie znaków**
  To ustawienie umożliwia włączanie lub wyłączanie optycznego rozpoznawania znaków (OCR) w celu wyodrębnienia — na potrzeby późniejszej inspekcji zawartości — fragmentów tekstu w 31 językach zapisanych z plików graficznych i obrazów w dokumentach, wiadomościach, skanach i zrzutach ekranu oraz innych obiektach.
- **Przesyłanie danych chronionych hasłem**
  Zawartości archiwów i dokumentów chronionych hasłem nie można sprawdzić. Za pomocą tego ustawienia usługa Advanced DLP umożliwia administratorowi określenie, czy wychodzące operacje przesyłania danych chronionych hasłem mają być dozwolone czy blokowane.
- **Zapobiegaj przesyłaniu danych w przypadku błędów**
  Czasami analiza przesyłanej zawartości może się nie powieść lub może wystąpić inny błąd kontroli w ramach operacji agenta zapobiegania utracie danych. W przypadku włączenia tej opcji w obliczu takich trudności operacja zostanie zablokowana. Jeśli opcja będzie wyłączona, operacja przesyłania zostanie wykonana mimo wystąpienia błędu.
- **Lista dozwolonych typów urządzeń i komunikacji sieciowej**
  Operacje przesyłania danych do zaznaczonych na tej liście typów urządzeń peryferyjnych i komunikacji sieciowej są dozwolone niezależnie od poufności danych i egzekwowanych zasad przepływów danych.

© Acronis International GmbH, 2003-2024

Ostrzeżenie!
Tej opcji należy używać w razie problemów z określonym typem urządzenia lub protokołem. Nie włączaj jej, dopóki nie zostanie to zalecone przez pracownika działu pomocy technicznej.

- **Lista dozwolonych hostów zdalnych**
  Operacje przesyłania danych do hostów docelowych wymienionych na tej liście są dozwolone niezależnie od poufności danych i egzekwowanych zasad przepływów danych.
- **Lista dozwolonych aplikacji**
  Operacje przesyłania danych wykonywane przez aplikacje wymienione na tej liście są dozwolone niezależnie od poufności danych i egzekwowanych zasad przepływów danych.

Wskaźnik **Poziom zabezpieczeń** w sekcji Ustawienia zaawansowane wyświetlanej w widoku **Utwórz plan ochrony** i w widoku „Szczegóły" planu ochrony działa zgodnie z następującą logiką wskazywania poziomu:

- **Podstawowy** — oznacza, że nie jest włączone żadne ustawienie zaawansowane.
- **Średni** — oznacza, że jest włączone co najmniej jedno ustawienie, ale nie aktywowano kombinacji opcji **Optyczne rozpoznawanie znaków**, **Przesyłanie danych chronionych hasłem** i **Zapobiegaj przesyłaniu danych w przypadku błędów**.
- **Rygorystyczny** — oznacza, że aktywowano co najmniej kombinację opcji **Optyczne rozpoznawanie znaków**, **Przesyłanie danych chronionych hasłem** i **Zapobiegaj przesyłaniu danych w przypadku błędów**.

Automatyczne wykrywanie miejsca docelowego

W trybie Obserwacja mieszana usługa Advanced Data Loss Prevention stosuje różne reguły, w zależności od miejsca docelowego wykrytego przesyłania danych — wewnętrznego lub zewnętrznego. Poniżej opisano logikę ustalania miejsca docelowego jako wewnętrznego. Wszystkie inne miejsca docelowe są uznawane za zewnętrzne.

W przypadku każdej przechwyconej operacji przesyłania danych usługa Advanced Data Loss Prevention automatycznie wykrywa, czy docelowy serwer HTTP, FTP lub SMB jest serwerem wewnętrznym, wykonując żądanie DNS i porównując nazwy FQDN komputera, na którym działa agent zapobiegania utracie danych, oraz serwera zdalnego. Jeśli żądanie DNS się nie powiedzie, usługa sprawdza też, czy chronione obciążenie i serwer zdalny znajdują się w tej samej sieci. Serwery mające tę samą nazwę domeny (czyli znajdujące się w tej samej podsieci) co komputer, na którym działa agent zapobiegania utracie danych, są uznawane za wewnętrzne.

W przypadku komunikacji e-mail usługa Advanced Data Loss Prevention traktuje jako przesyłanie wewnętrzne wszystkie wiadomości e-mail wysyłane z firmowego adresu e-mail przy użyciu firmowego serwera poczty, jeśli adres e-mail adresata znajduje się w tej samej domenie co adres e-mail nadawcy i nazwa serwera poczty adresata jest taka sama.

E-maile pozafirmowe są traktowane jako komunikacja zewnętrzna, chyba że konto odbiorcy jest znane. Znane adresy e-mail są aktualizowane, ponieważ usługa Zapobieganie utracie danych

© Acronis International GmbH, 2003-2024

monitoruje działania użytkowników w sieci i aktualizuje bazę danych na zapleczu przy użyciu danych adresów e-mail skojarzonych z danym użytkownikiem.

Komunikacja za pośrednictwem komunikatorów jest traktowana jako komunikacja zewnętrzna, chyba że jest znane konto odbiorcy. Znane konta są aktualizowane, ponieważ usługa Zapobieganie utracie danych monitoruje działania użytkowników w sieci i aktualizuje bazę danych na zapleczu przy użyciu danych kont skojarzonych z danym użytkownikiem.

Definicje poufnych danych

W tym temacie opisano logikę identyfikowania poufnych danych podczas analiz zawartości.

Aby zmniejszyć liczbę wyników fałszywie dodatnich, identyczne dopasowania są liczone jako jedno dopasowanie w przypadku wszystkich grup opisanych wyrażeń logicznych.

Ważne
Wyrażenia logiczne używane do identyfikowania zawartości mają charakter wyłącznie informacyjny i nie opisują rozwiązania w sposób szczegółowy.

Chronione informacje dotyczące zdrowia (PHI)

Obsługiwane języki

- Angielski amerykański, angielski brytyjski, angielski — międzynarodowy
- Fiński
- Włoski
- Francuski
- Polski
- Rosyjski
- Węgierski
- Norweski
- Hiszpański

Dane uznawane za chronione informacje dotyczące zdrowia

Poniższe dane są uznawane za chronione informacje dotyczące zdrowia.

- Imię i nazwisko
- Adres (ulica i numer budynku, miejscowość, województwo, okręg wyborczy, kod pocztowy i odpowiadające im identyfikatory geograficzne)
- Numer telefonu
- Adres e-mail
- PESEL

© Acronis International GmbH, 2003-2024

- Numer beneficjenta ubezpieczenia zdrowotnego
- Numer konta bankowego
- Adresy URL
- Numery adresów IP
- Kody ICD-10-CM
- ICD-10-PCS-and-GEMs
- HIPAA
- Inne dane dotyczące opieki zdrowotnej
- Numer karty kredytowej

Wyrażenie logiczne używane w celu wykrywania zawartości

Wyrażenie logiczne składa się z następujących ciągów połączonych operatorem logicznym OR. Operator OR jest używany do łączenia różnych grup danych z powyższej listy, jeśli operator logiczny AND nie zostanie jawnie określony. Liczba w nawiasie oznacza liczbę wykrytych instancji, które spowodowałyby dodatni wynik wykrywania.

- **PESEL** (5)
- (Imię i nazwisko (3) OR Adres (3) OR Numer telefonu (3) OR Adres e-mail (3) OR Numer konta bankowego (3) OR Numer karty kredytowej (3)) AND (PESEL (3) OR Numer beneficjenta ubezpieczenia zdrowotnego (3) * OR Kody ICD-10-CM (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR * Inne dane dotyczące opieki zdrowotnej (3))

Dane osobowe (PII)

Obsługiwane języki

- Angielski amerykański, angielski brytyjski, angielski — międzynarodowy
- Bułgarski
- Chiński
- Czeski
- Duński
- Holenderski
- Fiński
- Francuski
- Niemiecki
- Węgierski
- Indonezyjski
- Włoski

© Acronis International GmbH, 2003-2024

- Koreański
- Malajski
- Norweski
- Polski
- Portugalski (brazylijski)
- Portugalski (portugalski)
- Rumuński
- Rosyjski
- Serbski
- Singapur
- Hiszpański
- Szwedzki
- Tajwan
- Turecki
- Tajski
- Japoński

Dane uznawane za dane osobowe (PII)

- Imię i nazwisko
- Adres (ulica i numer budynku, miejscowość, województwo, kod pocztowy)
- Numer konta bankowego
- Identyfikator osobisty lub podatkowy
- Numer paszportu
- PESEL
- Numer telefonu
- Numer rejestracyjny pojazdu
- Numer dowodu osobistego
- Identyfikator i numer seryjny
- Adresy IP
- Adres e-mail
- Numer karty kredytowej

© Acronis International GmbH, 2003-2024

Wyrażenie logiczne używane w celu wykrywania zawartości

Wyrażenie logiczne w przypadku wszystkich obsługiwanych języków z wyjątkiem japońskiego

Wyrażenie logiczne składa się z następujących ciągów połączonych operatorem logicznym OR lub AND. Liczba w nawiasie oznacza liczbę wykrytych instancji, które spowodowałyby dodatni wynik wykrywania.

- Identyfikator osobisty lub podatkowy (5)
- Imię i nazwisko (3) AND **(**Numer karty kredytowej (3) OR PESEL (3) OR Numer konta bankowego (3) OR Identyfikator osobisty lub podatkowy (3) OR Numer dowodu osobistego (3) OR Numer paszportu (3) OR PESEL (3) OR Adresy IP (3) OR Numer rejestracyjny pojazdu (3) OR Identyfikator i numer seryjny**)**
- Numer telefonu (3) AND **(**Numer karty kredytowej (3) OR PESEL (3) OR Numer konta bankowego (3) OR Adres (3) OR Identyfikator osobisty lub podatkowy (3) OR Numer dowodu osobistego (3) OR Numer paszportu (3) OR PESEL (3) OR Numer rejestracyjny pojazdu (3) OR Identyfikator i numer seryjny (3)**)**
- **(**Imię i nazwisko (30) OR Adres (30)**)** AND **(**Adres e-mail (30) OR Numer telefonu (30) OR Adres IP (30)**)**
- Adres e-mail (3) AND **(**Numer karty kredytowej (3) OR PESEL (3) OR Numer konta bankowego (3) OR Identyfikator osobisty lub podatkowy (3) OR Numer dowodu osobistego (3) OR Numer paszportu (3) OR PESEL (3) OR Numer rejestracyjny pojazdu (3) OR Identyfikator i numer seryjny (3)**)**
- Adres e-mail (30) AND **(**Adres (30) OR Numer telefonu (30)**)**
- Imię i nazwisko (30) AND Adres (30)
- Numer telefonu (30) AND Adres (30)
- Imię i nazwisko (3) AND Numer konta bankowego (3)
- Numer telefonu (3) AND **(**Numer karty kredytowej (3) OR Numer konta bankowego (3) OR PESEL (3) OR Identyfikator osobisty lub podatkowy (3) OR Numer dowodu osobistego (3) OR Numer paszportu (3)**)**

Wyrażenie logiczne dla języka japońskiego

Uwaga
W procesie wykrywania zawartości zliczane są tylko unikatowe dopasowania.

Wyrażenie logiczne składa się z następujących ciągów połączonych operatorem logicznym OR. Operator OR jest używany do łączenia różnych grup, jeśli operator logiczny AND nie zostanie jawnie określony.

© Acronis International GmbH, 2003-2024

- PESEL (5)
- Imię i nazwisko (3) AND **(**Numer karty kredytowej (3) OR Numer konta bankowego (3) OR Numer dowodu osobistego (3) OR Numer paszportu (3) OR PESEL (3)**)**
- Imię i nazwisko (30) AND **(**Adres e-mail (30) OR Numer telefonu (30) OR Adres IP (30) OR Adres (30)**)**
- Adres (3) AND **(**Numer karty kredytowej (3) OR Numer konta bankowego (3) OR Numer dowodu osobistego (3) OR Numer paszportu (3) OR PESEL (3)**)**
- Adres e-mail (3) AND **(**Numer karty kredytowej (3) OR Numer konta bankowego (3) OR PESEL (3) OR Numer dowodu osobistego (3)**)**
- Adres (5) AND **(**Adres e-mail (5) OR Imię i nazwisko (5) OR Numer telefonu (5) OR Adres IP (5)**)**
- Imię i nazwisko (3) AND Numer konta bankowego (3)
- Numer telefonu (3) AND **(**Numer karty kredytowej (3) OR Numer konta bankowego (3) OR Adres (3) OR PESEL (3) OR Numer dowodu osobistego (3)**)**

Norma bezpieczeństwa danych w branży kart płatniczych (PCI DSS)

Obsługiwane języki

W tej grupie poufności nie występują żadne zależności od języka. Dane PCI DSS we wszystkich krajach są zapisywane w języku angielskim.

Dane uznawane za PCI DSS

- Dane posiadacza karty kredytowej
  - Numer karty (PAN)
  - Imię i nazwisko posiadacza karty
  - Data wygaśnięcia
  - Kod usługi
- Wrażliwe dane uwierzytelniające
  - Dane zapisane na karcie (dane na pasku magnetycznym lub jego odpowiedniku w postaci mikroukładu)
  - CAV2/CVC2/CVV2/CID
  - Kod PIN / blokada PIN

Wyrażenie logiczne używane w celu wykrywania zawartości

Wyrażenie logiczne składa się z następujących ciągów połączonych operatorem logicznym OR. Liczba w nawiasie oznacza liczbę wykrytych instancji, które spowodowałyby dodatni wynik wykrywania.

© Acronis International GmbH, 2003-2024

- Numer karty kredytowej (5)
- Numer karty kredytowej (3) AND (Amerykańskie imię i nazwisko (Ex) (3) OR Amerykańskie imię i nazwisko (3) OR Słowa kluczowe PCI DSS (3) OR Data (miesiąc/rok) (3))
- Zrzut karty kredytowej (5)

Oznaczono jako poufne

Dane oznaczone jako poufne są wykrywane za pomocą grupy słów kluczowych.

Warunek dopasowania opiera się na wadze, przy czym każde słowo ma wagę == 1. Wykrycie zawartości jest uznawane za dodatnie, gdy waga dopasowania > 3.

Obsługiwane języki

- Angielski
- Bułgarski
- Chiński uproszczony
- Chiński tradycyjny
- Czeski
- Duński
- Holenderski
- Fiński
- Francuski
- Niemiecki
- Węgierski
- Indonezyjski
- Włoski
- Japoński
- Koreański
- Malajski
- Norweski
- Polski
- Portugalski — brazylijski
- Portugalski — portugalski
- Rosyjski
- Serbski
- Hiszpański

© Acronis International GmbH, 2003-2024

- Szwedzki
- Turecki

Grupy słów kluczowych

Grupa słów kluczowych w przypadku każdego języka zawiera specyficzne dla danego kraju odpowiedniki następujących słów kluczowych, które są używane w języku angielskim (wielkość liter nie ma znaczenia).

- poufne
- dystrybucja wewnętrzna
- nie do rozpowszechniania
- nie rozpowszechniać
- nie do wiadomości publicznej
- nie do rozpowszechniania poza firmą
- tylko do użytku wewnętrznego
- ściśle tajna dokumentacja
- nieoficjalne
- informacje niejawne
- tylko do użytku wewnętrznego
- tylko do użytku oficjalnego

Zdarzenia funkcji Zapobieganie utracie danych

Usługa Advanced Data Loss Prevention generuje zdarzenia w widoku zdarzeń funkcji Zapobieganie utracie danych w niżej opisany sposób.

- W trybie obserwacji zdarzenia są generowane w przypadku wszystkich uzasadnionych operacji przesyłania danych.
- W trybie egzekwowania zdarzenia są generowane z uwzględnieniem czynności **Zapisz w dzienniku** skonfigurowanej dla każdej wyzwolonej reguły.

Aby wyświetlić zdarzenia dla reguły przepływu danych

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Ochrona** > **Zasady przepływów danych**.
3. Znajdź regułę, dla której chcesz wyświetlić zdarzenia, i kliknij wielokropek na końcu wiersza reguły.
4. Wybierz **Wyświetl zdarzenia**.

© Acronis International GmbH, 2003-2024

Aby wyświetlić szczegółowe informacje o zdarzeniu w widoku zdarzeń funkcji Zapobieganie utracie danych

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Ochrona** > **Zdarzenia funkcji Zapobieganie utracie danych**.
3. Kliknij zdarzenie na liście, aby wyświetlić więcej szczegółów na jego temat.
   Po prawej stronie zostanie wyświetlone okienko Szczegóły zdarzenia.
4. W okienku Szczegóły zdarzenia przewijaj w dół i w górę, aby wyświetlić dostępne informacje.
   Szczegóły wyświetlane w tym okienku zależą od typu i ustawień reguły, która wyzwoliła zdarzenie.

Aby przefiltrować listę zdarzeń funkcji Zapobieganie utracie danych

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Ochrona** > **Zdarzenia funkcji Zapobieganie utracie danych**.
3. Kliknij **Filtruj** w lewym górnym rogu.
4. Wybierz z menu rozwijanych kategorię poufności, obciążenie, typ czynności, użytkownika i kanał.
   W menu rozwijanym można wybrać więcej niż jedną pozycję. Podczas filtrowania między pozycjami z tego samego menu jest stosowany operator logiczny OR, a między pozycjami z różnych menu jest stosowany operator logiczny AND.
   Jeśli na przykład wybierzesz kategorie poufności **PHI** i **PII**, w wynikach będą wyświetlane wszystkie zdarzenia, które zawierają informacje PHI (o stanie zdrowia), informacje PII (dane osobowe) lub oba te rodzaje informacji. Jeśli wybierzesz kategorię poufności **PHI** i czynność **Dostęp do zapisu**, w wynikach filtrowania będą wyświetlane tylko zdarzenia pasujące do obu kategorii.
5. Kliknij **Zastosuj**.
6. Aby ponownie wyświetlić wszystkie zdarzenia, kliknij kolejno **Filtruj**, **Przywróć domyślne** i **Zastosuj**.

Aby wyszukać zdarzenia na liście zdarzeń funkcji Zapobieganie utracie danych

1. Powtórz kroki 1–2 powyższej procedury.
2. Z listy rozwijanej po prawej stronie pola Filtruj wybierz kategorię, w której chcesz przeprowadzić wyszukiwanie: **Nadawca**, **Miejsce docelowe**, **Proces**, **Temat wiadomości** lub **Powód**.
3. W polu tekstowym wpisz interesujące Cię hasło i potwierdź przez naciśnięcie klawisza Enter.
   Na liście będą wyświetlane tylko zdarzenia pasujące do wprowadzonego hasła.
4. Aby zresetować listę zdarzeń, kliknij znak **X** w polu tekstowym wyszukiwania i naciśnij klawisz Enter.

Aby wyświetlić listę zdarzeń związanych z określonymi regułami przepływów danych

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Ochrona** > **Zasady przepływów danych**.

© Acronis International GmbH, 2003-2024

3. Zaznacz pole wyboru dostępne przed nazwą interesującej Cię reguły.
   W razie potrzeby możesz zaznaczyć wiele reguł.
4. Kliknij **Wyświetl zdarzenia**.
   Zostanie otwarty widok **Ochrona** > **Zdarzenia funkcji Zapobieganie utracie danych** i lista zdarzeń związanych z wybranymi regułami.

Widżety usługi Advanced Data Loss Prevention na pulpicie nawigacyjnym Przegląd

Pulpit nawigacyjny **Przegląd** udostępnia szereg dostosowywanych widżetów zapewniających ogólny obraz operacji związanych z rozwiązaniem Cyber Protection, w tym usługą Advanced Data Loss Prevention. Na pulpicie nawigacyjnym **Przegląd**, w obszarze **Monitorowanie**, można znaleźć niżej wymienione widżety usługi Advanced Data Loss Prevention.

- **Przesyłanie poufnych danych** — umożliwia wyświetlenie łącznej liczby operacji przesyłania poufnych danych do odbiorców wewnętrznych i zewnętrznych. Zestawienie jest podzielone według typu uprawnień: dozwolone, uzasadnione lub zablokowane. Widżet ten można dostosować do własnych potrzeb, wybierając żądany zakres czasu (1 dzień, 7 dni, 30 dni lub Ten miesiąc).
- **Kategorie wychodzących poufnych danych** — umożliwia wyświetlenie łącznej liczby operacji przesyłania poufnych danych do odbiorców zewnętrznych. Zestawienie jest podzielone według kategorii poufności: Chronione informacje dotyczące zdrowia (PHI), Dane osobowe (PII), PCI DSS i Oznaczono jako poufne (Poufne).
- **Czołowi nadawcy wychodzących poufnych danych** — umożliwia wyświetlenie łącznej liczby operacji przesyłania poufnych danych z organizacji do odbiorców zewnętrznych oraz listy 5 użytkowników z największą liczbą operacji przesyłania (wraz z tą liczbą w przypadku każdego z nich). W statystyce są uwzględniane dozwolone i uzasadnione operacje przesyłania. Widżet ten można dostosować do własnych potrzeb, wybierając żądany zakres czasu (1 dzień, 7 dni, 30 dni lub ten miesiąc).
- **Czołowi nadawcy zablokowanych operacji przesyłania poufnych danych** — umożliwia wyświetlenie łącznej liczby zablokowanych operacji przesyłania poufnych danych oraz listy 5 użytkowników z największą liczbą podjętych prób przeprowadzenia operacji przesyłania (wraz z tą liczbą w przypadku każdego z nich). Widżet ten można dostosować do własnych potrzeb, wybierając żądany zakres czasu (1 dzień, 7 dni, 30 dni lub Ten miesiąc).
- **Ostatnie zdarzenia DLP** — umożliwia wyświetlenie szczegółowych informacji o ostatnich zdarzeniach związanych z zapobieganiem utracie danych w wybranym zakresie czasu. Widżet ten można dostosować przy użyciu następujących opcji:
  - **Zakres (data publikacji)** (1 dzień, 7 dni, 30 dni lub Ten miesiąc)
  - Nazwa **obciążenia**
  - **Status operacji** (dozwolona, uzasadniona lub zablokowana)
  - **Poziom poufności** (PHI, PII, Poufne, PCI DSS)

© Acronis International GmbH, 2003-2024

- **Typ miejsca docelowego** (zewnętrzne, wewnętrzne)
- **Grupowanie** (obciążenie, użytkownik, kanał, typ miejsca docelowego)

Widżety są aktualizowane co 5 minut. Widżety mają klikalne elementy, które pozwalają badać i rozwiązywać problemy. Możesz pobrać bieżący stan pulpitu nawigacyjnego lub przesłać go za pomocą poczty e-mail w formacie .pdf oraz/lub .xlsx.

Niestandardowe kategorie poufności

Niestandardowe kategorie poufnych danych mogą pomóc organizacji chronić własność intelektualną i poufne dane charakterystyczne dla tej organizacji przez rozszerzenie wbudowanego w moduł Advanced DLP katalogu definicji zawartości związanych z regulacjami dotyczącymi zgodności z wymogami.

Aby utworzyć niestandardową kategorię poufności

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Klasyfikatory danych**.
3. Wybierz **Kategoria poufności**.
4. Zostanie wyświetlona lista poziomów poufności, zarówno wbudowanych (takich jak Chronione informacje dotyczące zdrowia czy Dane osobowe), jak i niestandardowych.
5. Kliknij **Utwórz poziom poufności** w prawym górnym rogu okna.
6. Wpisz jego nazwę w nowo otwartym oknie.
7. Nowe niestandardowe poziomy poufności są zawsze domyślnie wyłączone. Można je włączyć po skonfigurowaniu wszystkich ich parametrów.
8. Utworzywszy nowy poziom poufności, trzeba skonfigurować jego detektory zawartości. Kliknij strzałkę, aby rozwinąć zawartość nowego poziomu poufności, i wybierz **Dodaj detektor zawartości**.
9. W następnym oknie możesz użyć dowolnego z już istniejących detektorów zawartości (w tym celu kliknij pola wyboru obok ich nazw, a następnie kliknij **Dodaj** w prawym dolnym rogu) lub zdefiniować nowy.
10. Zamiast tworzyć nowy poziom poufności od zera, możesz wykorzystać poziom już istniejący (wbudowany lub niestandardowy) — wystarczy go sklonować i dostosować jego parametry.
    - Aby sklonować już istniejący poziom poufności, kliknij pole wyboru obok jego nazwy, a następnie wybierz **Klonuj** z menu rozwijanego Czynność (oznaczonego wielokropkiem) w lewym górnym rogu. Jeśli chcesz sklonować więcej niż jeden poziom poufności, możesz zaznaczyć wiele pozycji naraz.
    - W następnym oknie możesz wybrać, które parametry danego poziomu poufności chcesz zachować, klikając pola wyboru obok każdego z nich.

© Acronis International GmbH, 2003-2024

Uwaga
Skopiowanie wbudowanych poziomów poufności w ramach jednego dzierżawcy powoduje utworzenie nowego poziomu poufności obejmującego te same detektory (po skopiowaniu będą detektorami niestandardowymi).

Aby utworzyć nowy detektor zawartości

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Klasyfikatory danych**.
3. Wybierz **Detektory zawartości**.
4. Zostanie wyświetlona lista detektorów zawartości, zarówno wbudowanych, jak i niestandardowych.
5. Kliknij **Utwórz detektor zawartości** w prawym górnym rogu okna.
6. Zostanie otwarte menu rozwijane, w którym można wybrać typ tworzonego detektora. Obecnie jest dostępny tylko detektor zawartości **Typ pliku**. W przyszłych aktualizacjach będą dodawane kolejne detektory.
7. W poniższym oknie można skonfigurować detektor zawartości.

Typ detektora zawartości	Opis
Detektor zawartości Typ pliku	a. Dostępne są dwie listy: **Obsługiwane typy plików** oraz **Wybrane typy plików**. Kliknięcie ikony „plus” po prawej stronie obsługiwanego typu pliku spowoduje przeniesienie go na listę Wybrane typy plików. Można też wybrać wiele obsługiwanych typów plików naraz — w tym celu należy kliknąć pola wyboru obok ich nazw, a następnie kliknąć **Dodaj wybrane** w prawym górnym rogu. b. Aby usunąć typ pliku z listy Wybrane typy plików, kliknij ikonę kosza po prawej stronie nazwy typu. Można też usunąć wiele typów plików naraz — w tym celu należy kliknąć odpowiadające im pola wyboru, a następnie przycisk **Usuń wybrane**.
Detektor zawartości Słowa kluczowe	a. Tworząc nowy detektor zawartości na potrzeby słów kluczowych należy zaimportować słowa kluczowe z pliku. Po pomyślnym imporcie można scalić nowe słowa kluczowe z listą już istniejących słów kluczowych lub zastąpić istniejące słowa kluczowe importowanymi. b. Trzeba też określić, czy detektor zawartości ma dopasowywać wszystkie słowa kluczowe z listy, dowolne słowo kluczowe z listy czy niestandardową liczbę słów kluczowych.

8. Zamiast tworzyć nowy detektor zawartości od zera, możesz wykorzystać detektor już istniejący (wbudowany lub niestandardowy) — wystarczy go sklonować i dostosować jego parametry.
   - Aby sklonować już istniejący detektor zawartości, kliknij pole wyboru obok jego nazwy, a następnie wybierz **Klonuj** z menu rozwijanego Czynność (oznaczonego wielokropkiem) w

© Acronis International GmbH, 2003-2024

lewym górnym rogu. Jeśli zechcesz sklonować więcej niż jeden detektor zawartości, możesz zaznaczyć wiele pozycji naraz.

Uwaga
Kopia wbudowanego detektora zawartości staje się detektorem niestandardowym.

Mapa organizacji

Uwaga
Ta funkcja jest dostępna tylko dla użytkowników z rolą Administrator firmy.

Mapa organizacji to baza danych zawierająca dane użytkowników i wszystkie ich konta używane do przesyłania danych za pośrednictwem komunikatorów, poczty e-mail lub w dowolny inny sposób, które zostały przechwycone przez moduł Advanced DLP.

Mapa organizacji umożliwia tworzenie grup użytkowników i zarządzanie nimi w module Advanced DLP, a także zarządzanie użytkownikami i kontami powiązanymi z użytkownikami w module Advanced DLP. Grupy użytkowników można następnie wykorzystywać do zarządzania zasadami DLP opartego na grupach.

Aby zlokalizować mapę organizacji

- W konsoli Cyber Protect Cloud przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Mapa organizacji**.

Jak to działa?

Uwaga
Mapa organizacji jest wypełniana, gdy moduł Advanced DLP działa w trybie Obserwacja.

W przypadku każdej transmisji danych przechwyconej przez agenta DLP, na zapleczu są gromadzone następujące atrybuty.

Atrybut	Opis	Etykieta w interfejsie użytkownika
Jednostka organizacyjna	Ręcznie utworzona grupa. Jednostka organizacyjna może mieć jedną lub więcej zagnieżdżonych jednostek organizacyjnych.	Nazwa grupy, zgodnie z definicją
Identyfikator zabezpieczeń	Unikatowy identyfikator zabezpieczeń.	Na stronie szczegółów użytkownika > **SID**
	Przyjazna dla użytkownika wyświetlana nazwa pochodząca od nazw kont użytkownika. Nazwa ta nie zawsze jest dostępna na	**Nazwa**

© Acronis International GmbH, 2003-2024

Atrybut	Opis	Etykieta w interfejsie użytkownika
	mapie organizacji.	
Komputer\Nazwa użytkownika	Nazwa użytkownika punktu końcowego (maszyny). Nazwę użytkownika można przypisać do tylko jednej jednostki organizacyjnej.	**Nazwa użytkownika**
Urządzenie (maszyna)	Nazwa punktu końcowego (maszyna).	**Obciążenie**
Konto	Konta, które były używane przez użytkownika do komunikacji za pośrednictwem komunikatorów oraz poczty e-mail i zostały przechwycone przez agenta DLP. Jeśli na przykład agent wykryje, że nazwa użytkownika „Komputer\John" używa do wysyłania wiadomości e-mail adresu john@gmail.com, to to konto jest powiązane z nazwą użytkownika Komputer\John.	**Konta**

Na mapie organizacji można przeglądać i wyszukiwać konta, użytkowników oraz grupy, a także tworzyć, edytować i usuwać grupy.

Aby wyszukać określone konta

W ramach dochodzenia w sprawie incydentu użytkownicy z rolą Administrator mogą potrzebować znaleźć właściciela konkretnego konta, które było zamieszane w potencjalne naruszenie bezpieczeństwa danych.

1. W konsoli Cyber Protect Cloud przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Mapa organizacji**.
2. W polu tekstowym **Szukaj** nad listą użytkowników zacznij wpisywać lub wklej nazwę konta.
   Lista jest filtrowana w trakcie pisania.

Aby wyszukać określoną nazwę użytkownika

1. W konsoli Cyber Protect Cloud przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Mapa organizacji**.
2. Aby szukać w określonej grupie, kliknij nazwę grupy na liście.
3. W polu tekstowym **Szukaj** nad listą użytkowników zacznij wpisywać lub wklej nazwę użytkownika.
   Lista jest filtrowana w trakcie pisania.

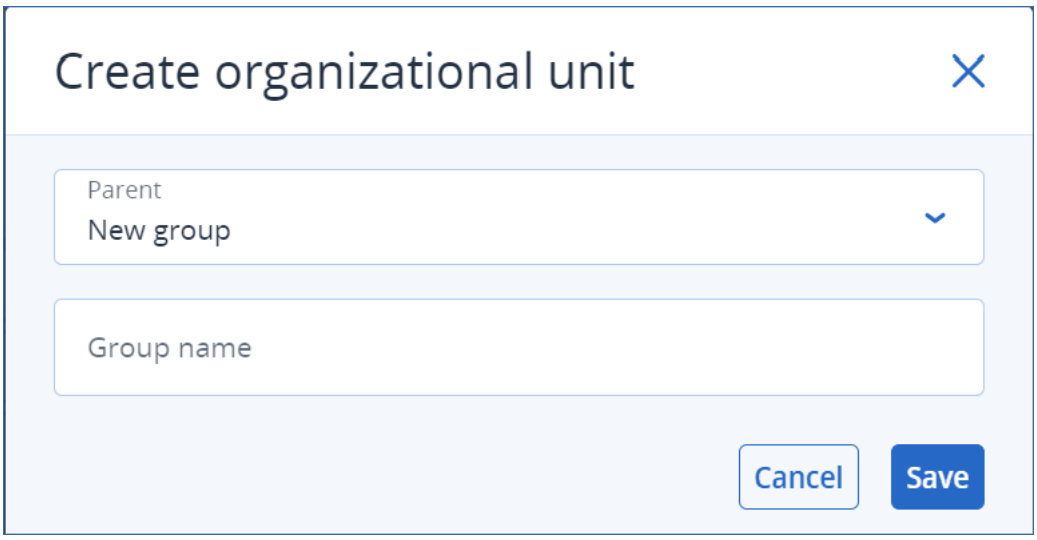
Aby wyświetlić konta używane przez określoną nazwę użytkownika

1. Znajdź użytkownika na liście użytkowników.
2. Kliknij trzy kropki na końcu wiersza użytkownika i wybierz **Widok**.
3. W oknie dialogowym szczegółów użytkownika znajdź sekcję **Powiązane konta**.
4. W polu tekstowym Opis można dodawać komentarze.

© Acronis International GmbH, 2003-2024

Aby utworzyć grupę użytkowników

1. W konsoli Cyber Protect Cloud przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Mapa organizacji**.
2. W lewej dolnej części listy grup kliknij **Utwórz grupę**.
   Zostanie otwarte okno dialogowe Utwórz jednostkę organizacyjną.



3. Z menu rozwijanego Element nadrzędny wybierz kontekst nowej grupy.

Uwaga
Elementu nadrzędnego nie można później zmienić. Grupa już pozostanie zagnieżdżona w tym kontekście.

4. Wprowadź nazwę grupy i kliknij **Zapisz**.

Aby dodać użytkownika do grupy

1. W konsoli Cyber Protect Cloud przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Mapa organizacji**.
2. Na liście użytkowników znajdź użytkownika, którego chcesz dodać, i zaznacz pole wyboru na początku wiersza użytkownika.
   Nad listą użytkowników pojawiają się przyciski **Przenieś wybrane** i **Usuń wybrane**.
3. Kliknij **Przenieś wybrane**.
   Zostanie otwarte okno dialogowe Przenieś użytkownika.
4. Wybierz nowy element nadrzędny dla wybranego użytkownika i kliknij **Zapisz**.

Uwaga
Użytkownik może należeć do tylko jednej grupy.

Aby usunąć konto powiązane z użytkownikiem

© Acronis International GmbH, 2003-2024

1. Znajdź użytkownika na liście użytkowników.
2. Kliknij trzy kropki na końcu wiersza użytkownika i wybierz **Widok**.
3. W oknie dialogowym szczegółów użytkownika znajdź sekcję **Powiązane konta**.
4. Znajdź konto, które chcesz usunąć, i kliknij trzy kropki obok niego.
5. Z listy rozwijanej wybierz **Usuń**.

Aby zmienić nazwę grupy użytkowników

1. W konsoli Cyber Protect Cloud przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Mapa organizacji**.
2. Kliknij trzy kropki obok nazwy grupy i kliknij **Zmień nazwę**.

Aby usunąć grupę użytkowników

1. W konsoli Cyber Protect Cloud przejdź do sekcji **Ochrona** > **Zapobieganie utracie danych** > **Mapa organizacji**.
2. Kliknij trzy kropki obok nazwy grupy i kliknij **Usuń**.
   Wszyscy użytkownicy z grupy zostają przeniesieni do jednostki nadrzędnej.

Znane problemy i ograniczenia

- [DEVLOCK-4028] W agencie pulpitu Zoom nie ma funkcji sterowania czatami grupowymi.
- [DEVLOCK-4016] Przyjazna nazwa i identyfikator nadawcy nie są przechwytywane na potrzeby GMX Web Mail i Web.de Mail w przypadku tworzenia wersji roboczej.
- [DEVLOCK-4447] Brak okna dialogowego Uzasadnienie na potrzeby naver.com WebMail w przypadku tworzenia wersji roboczej.
- [DEVLOCK-1033] DeviceLockDriver: potencjalna kontrola błędów DRIVER_POWER_STATE_FAILURE powodowana przez zakleszczenie podczas przetwarzania instrukcji IRP_MN_QUERY_DEVICE_RELATIONS.

Endpoint Detection and Response (EDR)

Uwaga
Funkcje te wchodzą w skład pakietu ochrony Zabezpieczenia zaawansowane + EDR, który z kolei stanowi część usługi Cyber Protection. Uwaga: w przypadku dodania funkcji EDR do planu ochrony mogą być naliczane dodatkowe opłaty.

Moduł EDR wykrywa podejrzane działania na obciążeniach, w tym ataki, które nie zostały zauważone. EDR następnie generuje incydenty, które zapewniają szczegółowy przegląd każdego ataku. Dzięki temu można łatwiej ustalić, jak doszło do ataku i jak można zapobiec jego ponownemu wystąpieniu. Dzięki przystępnym interpretacjom każdego etapu ataku dochodzenie w jego sprawie zajmuje znacznie mniej czasu — staje się kwestią minut.

© Acronis International GmbH, 2003-2024

Dlaczego potrzebne jest rozwiązanie Endpoint Detection and Response (EDR)

W obecnej sytuacji nieustająco narastających cyberzagrożeń i złośliwych ataków prewencja już nie gwarantuje stuprocentowej ochrony. Niektóre ataki wciąż będą pokonywać warstwy zapobiegawcze i skutecznie przenikać do sieci. Konwencjonalne rozwiązania nie wykrywają takich zdarzeń, co zapewnia hakerom swobodę penetrowania danego środowiska przez całe dni, tygodnie, a nawet miesiące.

Dotychczasowe rozwiązania EDR pomagają zapobiegać tym „cichym porażkom" dzięki szybkiemu wykrywaniu i usuwaniu skutków działań hakerów. Zwykle jednak wymagają dużej wiedzy z zakresu bezpieczeństwa lub drogich usług analityków z centrum operacji z zakresu bezpieczeństwa (Security Operation Center, SOC), a analiza incydentów potrafi być niezwykle czasochłonna.

Funkcje pakietu Zabezpieczenia zaawansowane + EDR firmy Acronis eliminują te ograniczenia dzięki wykrywaniu dotąd niezauważonych ataków, a jednocześnie pomagają ustalić, jak doszło do danego ataku i jak można zapobiec jego ponownemu wystąpieniu. To z kolei przekłada się na krótszy czas dochodzenia wyjaśniającego atak.

Oto dlaczego trzeba mieć rozwiązanie EDR:

- **Pełny wgląd**: dostęp do informacji o tym, co się wydarzyło i jak do tego doszło — nawet w przypadku dotychczas niezauważonych ataków. Ewolucja każdego ataku jest też wizualnie odwzorowana krok po kroku (od punktu wniknięcia do środowiska po przeglądanie danych, które były celem ataku i/lub zostały eksfiltrowane), co pozwala szybko ustalić zakres i skutki incydentu. Aby uzyskać więcej informacji, zobacz "Jak poddać incydenty dochodzeniu w cybernetycznym łańcuchu zabijania" (s. 986).
- **Minimalny czas trwania dochodzenia**: czas dochodzenia w sprawie incydentu zostaje skrócony z godzin do zaledwie minut. EDR udostępnia szczegółowe informacje o każdym etapie ataku w przystępnym, zrozumiałym dla człowieka języku, dzięki czemu ogranicza konieczność korzystania z usług drogich ekspertów lub dodatkowych pracowników. Dodatkowe informacje można znaleźć w sekcji "Poddawanie incydentów dochodzeniu" (s. 985).
- **Sprawdzanie obciążeń pod kątem występowania znanych zagrożeń**: obciążenia mogą być automatycznie przeszukiwane pod kątem zagrożeń powodowanych przez złośliwe oprogramowanie, luki w zabezpieczeniach i innego typu globalne zdarzenia, które mogą mieć ujemny wpływ na ochronę danych. Zagrożenia te nazywane są wskaźnikami naruszenia zabezpieczeń (Indicator of Compromise, IOC), a ich identyfikacja opiera są na danych o zagrożeniach otrzymywanych z Cyber Protection Operations Center (CPOC). Aby uzyskać więcej informacji, zobacz "Sprawdzanie obciążeń pod kątem występowania wskaźników naruszenia zabezpieczeń (IOC) z publicznie znanych ataków" (s. 998).
- **Szybsze reagowanie na incydenty**: mając dostęp do wszystkich działań, które warto wykonać po złamaniu zabezpieczeń środowiska, oraz dogłębne informacje o każdym etapie w ramach łańcucha zabijania, można wykonać szereg czynności mających na celu naprawienie skutków ataku w każdym jego punkcie. Można między innymi przeprowadzić dochodzenie z

© Acronis International GmbH, 2003-2024

wykorzystaniem technologii zdalnego sterowania i kopii zapasowych na potrzeby analizy śledczej (funkcja niedostępna w wersji Early Access), poddać obciążenia kwarantannie i zabić procesy złośliwego oprogramowania. Można też przywrócić operacje biznesowe za pomocą narzędzia Cyber Disaster Recovery Cloud. Aby uzyskać więcej informacji, zobacz "Naprawianie incydentów" (s. 1002).

- **Rzetelne raporty o ogólnym poziomie bezpieczeństwa środowiska**: włączenie modułu EDR pozwala pozbyć się wielu niepewności i obaw związanych z wpływem ataków cybernetycznych na działalność firmy. Ponadto informacje dotyczące incydentów są przechowywane przez 180 dni, co można wykorzystać do celów inspekcji.

Funkcje

Moduł Endpoint Detection and Response (EDR) obejmuje następujące funkcje:

- Generowanie alertów, gdy dojdzie do złamania zabezpieczeń
- Zarządzanie incydentami na stronie Incydenty
- Przystępne wizualizacje przebiegu ataku
- Zalecenia i kroki naprawcze
- Sprawdzanie obciążeń pod kątem wystąpienia ujawnionych publicznie ataków za pomocą kanałów dotyczących zagrożeń
- Krótki przegląd na pulpicie nawigacyjnym
- Przechowywanie zdarzeń związanych z bezpieczeństwem przez 180 dni

Generowanie alertów, gdy dojdzie do złamania zabezpieczeń

Moduł EDR generuje alerty po każdym wystąpieniu incydentu. Alerty te są wyróżniane w menu głównym konsoli Cyber Protect. Taki alert można następnie poddać dochodzeniu, klikając przycisk **Poddaj incydent dochodzeniu**, co spowoduje przekierowanie do ekranu dochodzenia w sprawie incydentu (nazywanego inaczej cybernetycznym łańcuchem zabijania).

Aby uzyskać więcej informacji, zobacz "Przeglądanie incydentów" (s. 964).

Zarządzanie incydentami na stronie Incydenty

Moduł EDR umożliwia zarządzanie wszystkimi incydentami na stronie Incydenty (dostęp z menu Ochrona w konsoli Cyber Protect). Strona Incydenty, którą można filtrować stosownie do wymagań, umożliwia szybkie i łatwe ustalanie bieżących statusów incydentów, w tym ich ważności, obciążeń, których dotyczy incydent, oraz poziomu prawdziwości. Można też przejść bezpośrednio do cybernetycznego łańcucha zabijania, aby poznać przebieg ataku — węzeł po węźle.

Dodatkowe informacje na temat strony Incydenty można znaleźć w sekcji "Przeglądanie incydentów" (s. 964).

© Acronis International GmbH, 2003-2024

Przystępne wizualizacje przebiegu ataku

Moduł EDR udostępnia wizualną prezentację ataku w bardzo czytelnej formie. Dzięki temu nawet osoby niezajmujące się ochroną bezpieczeństwa mogą bez trudu ustalić cele i ważność każdego ataku. Wcale nie trzeba korzystać z usług centrum operacji z zakresu bezpieczeństwa (SOC) ani zatrudniać ekspertów ds. bezpieczeństwa — moduł EDR udostępnia informacje o tym, jak dokładnie przebiegał atak, w tym:

- Jak haker dostał się do środowiska
- Jak zatarł swoje ślady
- Jakie szkody zostały wyrządzone
- Jak rozprzestrzeniał się atak

Aby uzyskać więcej informacji, zobacz "Jak poddać incydenty dochodzeniu w cybernetycznym łańcuchu zabijania" (s. 986).

Zalecenia i kroki naprawcze

Moduł EDR udostępnia jasne i proste do zrealizowania zalecenia dotyczące wyeliminowania skutków ataku na obciążenie. Aby szybko się uporać z atakiem, kliknij **Napraw cały incydent**, aby wyświetlić zalecane działania mające na celu zniwelowanie skutków incydentu. Te zalecane działania umożliwiają szybkie wznowienie operacji, na które wpłynął atak. Jeśli jednak zechcesz podjąć bardziej precyzyjne kroki naprawcze, możesz przejść do każdego węzła z osobna i naprawić problemy z zastosowaniem odpowiedniej czynności.

Aby uzyskać więcej informacji, zobacz "Naprawianie incydentów" (s. 1002).

Sprawdzanie obciążeń pod kątem wystąpienia ujawnionych publicznie ataków za pomocą kanałów dotyczących zagrożeń

Moduł EDR umożliwia między innymi przeglądanie obciążeń pod kątem już gdzieś przeprowadzonych, znanych ataków, które udokumentowano w kanałach dotyczących zagrożeń. Kanały dotyczące zagrożeń są generowane automatycznie na podstawie danych o zagrożeniach pozyskiwanych z Cyber Protection Operations Center (CPOC). Moduł EDR umożliwia sprawdzenie, czy takie zagrożenie wywarło negatywny wpływ na obciążenie, a następnie podjęcie niezbędnych kroków w celu wyeliminowania zagrożenia.

Aby uzyskać więcej informacji, zobacz "Sprawdzanie obciążeń pod kątem występowania wskaźników naruszenia zabezpieczeń (IOC) z publicznie znanych ataków" (s. 998).

Krótki przegląd na pulpicie nawigacyjnym

Moduł EDR udostępnia różne statystyki na pulpicie nawigacyjnym konsoli Cyber Protect. Widoczne są następujące informacje:

© Acronis International GmbH, 2003-2024

- Bieżący status zagrożenia, w tym liczba incydentów wymagających dochodzenia.
- Ewolucja ataków z uwzględnieniem ich ważności, a także sygnały dotyczące ewentualnych kampanii ataków.
- Wskaźnik skuteczności zamykania incydentów.
- Najbardziej ukierunkowane taktyki używane do ataków na Twoich klientów.
- Status sieci obciążenia: czy jest ono odizolowane, czy połączone.

Przechowywanie zdarzeń związanych z bezpieczeństwem przez 180 dni

Moduł EDR gromadzi zdarzenia związane z obciążeniami oraz aplikacjami i przechowuje je przez 180 dni. Zdarzenia sprzed 180 dni są usuwane (usuwanie zdarzeń odbywa się na podstawie ich wieku, a nie miejsca zajmowanego w pamięci masowej). Uwaga: nawet jeśli moduł EDR zostanie wyłączony, wszystkie wcześniej zgromadzone zdarzenia dotyczące obciążenia są nadal przechowywane i będą dostępne na potrzeby dochodzenia w sprawie incydentu.

Wymagania dotyczące oprogramowania

Moduł Endpoint Detection and Response (EDR) obsługuje następujące systemy operacyjne:

- Microsoft Windows 7 Service Pack 1 lub nowszy
- Microsoft Windows Server 2008 R2 lub nowszy

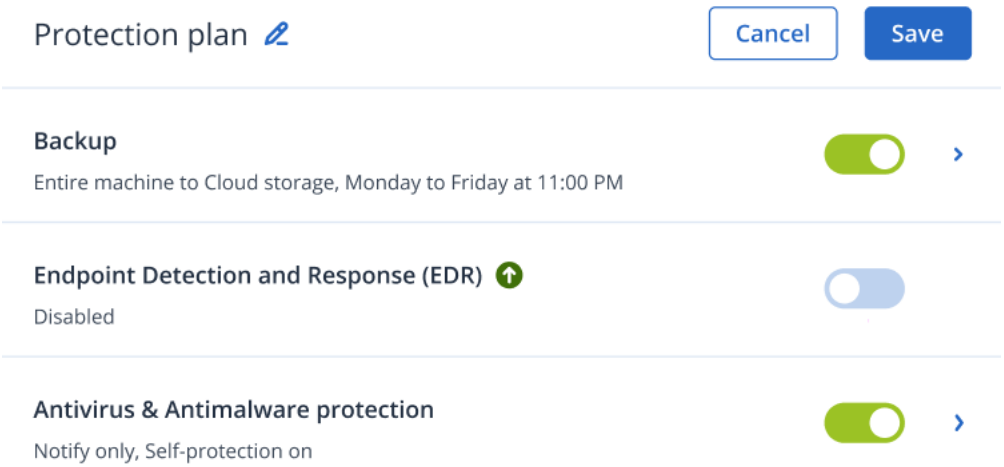
Włączanie funkcji modułu Endpoint Detection and Response (EDR)

Moduł EDR można włączyć w każdym planie ochrony.

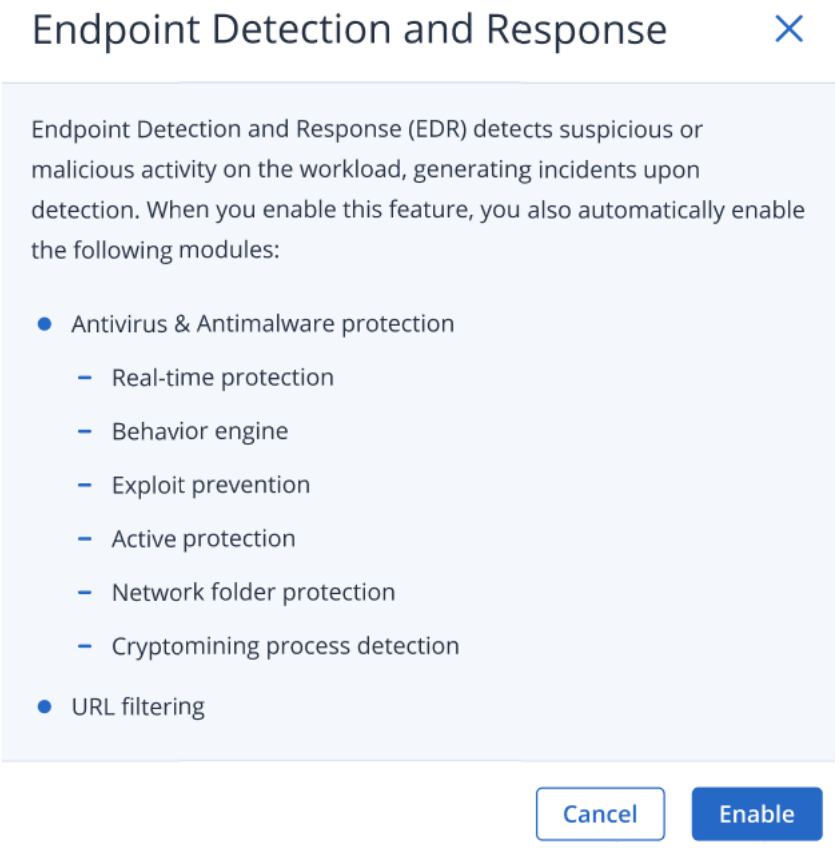
Aby włączyć moduł EDR

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie > Plany ochrony**.
2. Wybierz z wyświetlonej listy odpowiedni plan ochrony, a następnie na prawym pasku bocznym kliknij **Edytuj**.
   Ewentualnie możesz utworzyć nowy plan ochrony i przejść do następnego kroku. Dodatkowe informacje na temat pracy z planami ochrony można znaleźć w sekcji "Plany ochrony i moduły" (s. 221).
3. Na pasku bocznym planu ochrony włącz moduł **Endpoint Detection and Response (EDR)**, klikając przełącznik obok nazwy modułu.

© Acronis International GmbH, 2003-2024



4. W wyświetlonym oknie dialogowym kliknij **Włącz**. Należy pamiętać, że w przypadku włączenia modułu EDR włączane są również inne moduły ochrony, jak widać w wyświetlonym oknie dialogowym.



Uwaga
Jeśli przełącznik pozycji **Active Protection**, **Mechanizm zachowań**, **Ochrona przed exploitami** lub **Filtrowanie adresów URL** zostanie przestawiony na ustawienie **Wył.**, przełącznik modułu **Endpoint Detection and Response (EDR)** również będzie mieć ustawienie **Wył.**

© Acronis International GmbH, 2003-2024

5. Jak widać poniżej, ikona pakietu **Zabezpieczenia zaawansowane + EDR** zostanie dodana do listy pakietów ochrony wymaganych do implementacji planu ochrony — zależy ona od wybranych pakietów dodatkowych.

Korzystanie z modułu pakietu Endpoint Detection and Response (EDR)

Moduł EDR umożliwia wykrywanie dotąd niezauważonych ataków, a także pomaga ustalić, jak doszło do danego ataku i jak można zapobiec jego ponownemu wystąpieniu. Dzięki przystępnym interpretacjom każdego etapu ataku dochodzenie w jego sprawie zajmuje znacznie mniej czasu — staje się kwestią minut.

W poniższej tabeli opisano ogólny przepływ pracy podczas korzystania z modułu EDR. Najpierw należy przejrzeć wszystkie nowe incydenty i nadać im priorytety, potem należy je poddać dokładniejszemu dochodzeniu, korzystając z cybernetycznego łańcucha zabijania, a następnie można podjąć odpowiednie czynności naprawcze.

Krok	Jak korzystać z modułu EDR
KROK 1. Przejrzyj incydenty	Na liście incydentów w module EDR: • Ustal ogólny poziom bezpieczeństwa organizacji: ile incydentów wymaga dochodzenia? • Sprawdź, które incydenty mają najbardziej krytyczne znaczenie i nadaj priorytety dochodzeniom z uwzględnieniem ważności incydentów. • Ustal, które incydenty są nowe lub trwają jakiś czas.
KROK 2. Poddaj incydenty dochodzeniu	W cybernetycznym łańcuchu zabijania w module EDR: • Ustal cele hakera i przyjrzyj się użytym technikom ataku. • Sprawdź stopień prawdopodobieństwa, że dany incydent rzeczywiście jest złośliwym atakiem. • Sprawdź, czy obciążenie nie stało się celem ataku uwzględnionego w kanale dotyczącym zagrożeń. • Sprawdź, jakie czynności w ramach reagowania już wykonano w kontekście danego incydentu.
KROK 3. Napraw skutki incydentów	W odpowiednich sekcjach czynności naprawczych w module EDR: • Szybko i łatwo napraw wszystkie skutki incydentu, stosując globalne czynności w ramach reagowania. • Napraw problemy w poszczególnych punktach ataku w ramach incydentu. • Wykonaj czynności zapobiegające rozprzestrzenianiu się ataku (lub przyszłym atakom) bądź jego negatywnemu oddziaływaniu na obciążenia, które jeszcze nie stały się celem działań hakera.

© Acronis International GmbH, 2003-2024

Przeglądanie incydentów

Moduł Endpoint Detection and Response (EDR) udostępnia listę incydentów, która obejmuje zarówno wykrycia zdarzenia zapobiegawcze (czyli złośliwe oprogramowanie), jak i wykrycia podejrzanych elementów dotyczące danego obciążenia. Lista incydentów udostępnia krótki przegląd wszystkich ataków i zagrożeń mających wpływ na Twoje obciążenia, w tym zagrożeń, które trzeba zniwelować.

Na podstawie listy incydentów można szybko ustalić:

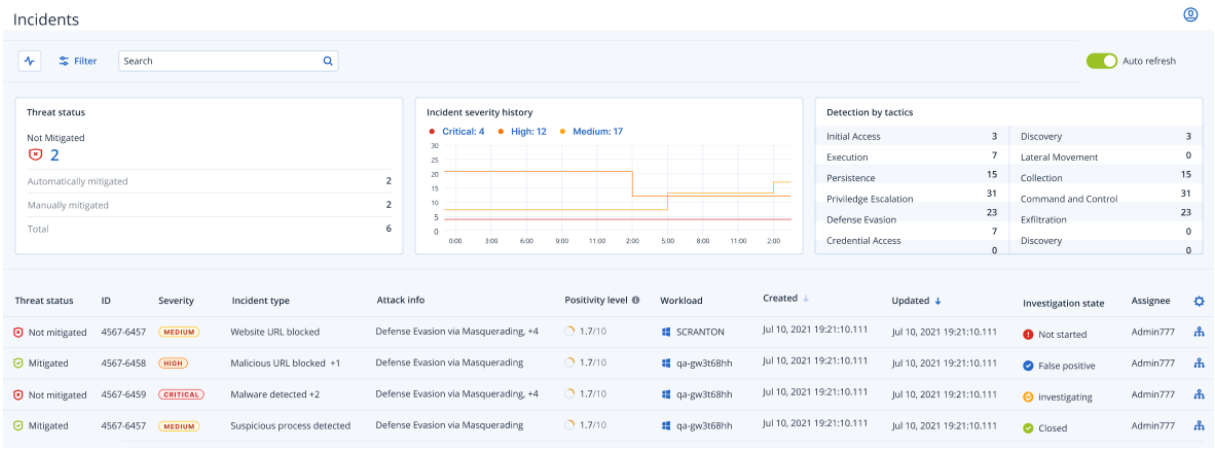
- Ogólny poziom bezpieczeństwa organizacji: ile incydentów wymaga dochodzenia?
- Które incydenty mają najbardziej krytyczne znaczenie — ponadto można nadać priorytet dochodzeniom z uwzględnieniem ważności incydentu.
- Które incydenty są nowe lub trwają jakiś czas.

Uwaga
Po zalogowaniu się jako administrator partnera możesz przeglądać wszystkie incydenty EDR na jednym ekranie, który zapewnia skonsolidowany widok incydentów wszystkich klientów bez uzyskiwania dostępu do indywidualnych widoków incydentów dotyczących poszczególnych klientów. Wyświetlana jest dodatkowa kolumna **Klienci**, zawierająca nazwę każdego klienta, z którym jest powiązany dany incydent. Ponadto widżety wyświetlane na pulpicie nawigacyjnym **Przegląd** zawierają zagregowane dane wskaźników dotyczące wszystkich klientów.

Jak widać poniżej, do listy incydentów można przejść z menu **Ochrona** w konsoli Cyber Protect. Dodatkowe informacje na temat przeglądania incydentów na liście incydentów można znaleźć w sekcji "Wyświetlanie incydentów, których skutków jeszcze nie zniwelowano" (s. 967). Więcej informacji o sytuacjach, w których jest tworzony incydent, można znaleźć w sekcji Czym dokładnie są incydenty?.

Uwaga
Jeśli na maszynach jest włączona usługa Zarządzane wykrywanie i reagowanie (Managed Detection and Response, MDR), jest też wyświetlana dodatkowa kolumna **Zgłoszenie usługi MDR**. W kolumnie tej jest wyświetlany numer zgłoszenia udostępniany przez dostawcę usługi Zarządzane wykrywanie i reagowanie.

© Acronis International GmbH, 2003-2024



Uwaga
Aby otrzymywać powiadomienia o incydentach, trzeba mieć otwartą konsolę Cyber Protect.

Czym dokładnie są incydenty?

Incydenty, czyli incydenty związane z bezpieczeństwem, można sobie wyobrazić jako *kontenery* z co najmniej jednym punktem wykrycia zapobiegawczego lub wykrycia podejrzanego elementu (bądź połączenia ich obu), a także wszystkimi powiązanymi incydentami i wykryciami dotyczącymi jednego ataku. Takie incydenty związane z bezpieczeństwem mogą też obejmować dodatkowe nieszkodliwe zdarzenia, które uzupełniają kontekst sytuacji.

Pozwala to na jednoczesne przeglądanie wszystkich zdarzeń związanych z atakiem w ramach jednego incydentu i poznanie logicznych kroków podjętych przez atakującego. Sprzyja też skróceniu czasu dochodzenia prowadzonego w sprawie ataku.

Jeśli moduł EDR jest włączony w planie ochrony, incydenty dotyczące bezpieczeństwa są tworzone, gdy:

- **Warstwa zapobiegawcza coś zatrzyma**: takie incydenty są automatycznie zamykane przez system zgodnie z ustawieniami planu ochrony. Można jednak przeprowadzić dochodzenie, co dokładnie zrobiło złośliwe oprogramowanie, zanim zostało zatrzymane. Na przykład oprogramowanie ransomware zostaje zatrzymane, gdy zaczyna szyfrować pliki, ale być może wcześniej wykradło poświadczenia lub zainstalowało jakąś usługę.
- **EDR wykryje podejrzane działania**: są to wykrycia, które powinny zostać poddane dochodzeniu i naprawione. Przeglądając wzbogacony o elementy wizualne cybernetyczny łańcuch zabijania (dodatkowe informacje można znaleźć w sekcji "Jak poddać incydenty dochodzeniu w cybernetycznym łańcuchu zabijania" (s. 986)), można łatwo zastosować odpowiednie działania naprawcze.

Nadawanie priorytetów incydentom wymagającym natychmiastowej uwagi

W każdej chwili można uzyskać dostęp do listy incydentów konsoli Cyber Protect z menu **Ochrona** w konsoli Cyber Protect. Lista incydentów udostępnia krótki przegląd wszelkich ataków i zagrożeń, a do tego umożliwia nadanie priorytetu incydentom wymagającym uwagi.

© Acronis International GmbH, 2003-2024

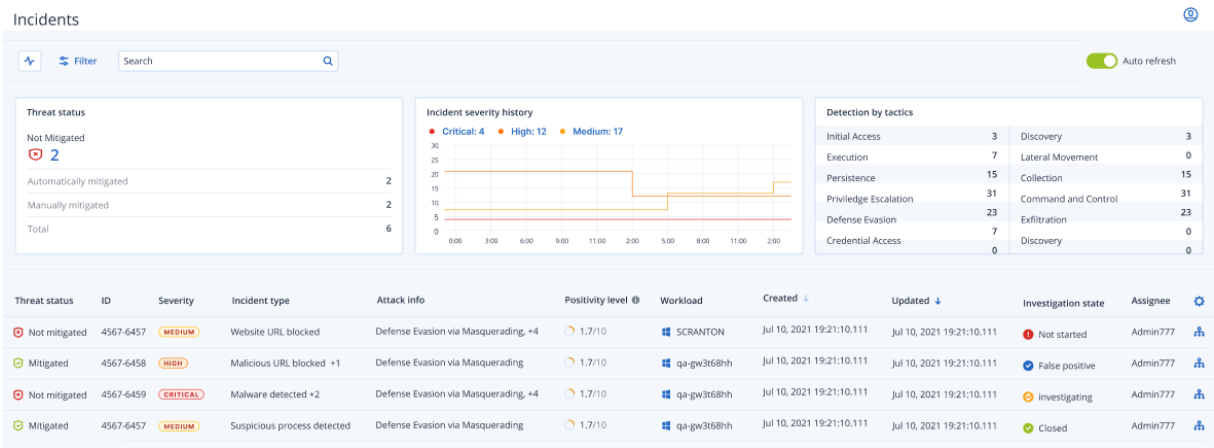
Ważne
Dbając o bezpieczeństwo obciążeń, *zawsze* analizuj incydenty i nadawaj priorytety tym z nich, które wciąż trwają lub których skutki wciąż nie zostały zniwelowane.

Jak przeanalizować, które incydenty naruszenia bezpieczeństwa niezwłocznie wymagają uwagi

Lista incydentów umożliwia analizowanie incydentów i nadawanie priorytetów tym z nich, które wymagają uwagi. Użytkownik może:

- Wyświetl incydenty, których skutków jeszcze nie zniwelowano: na podstawie listy incydentów szybko ustalisz, czy obecnie są prowadzone jakieś ataki. Wszelkie incydenty, których skutki nie zostały zniwelowane, co widać w kolumnie **Status zagrożeń**, powinny niezwłocznie zostać przejrzane (incydenty te są domyślnie wyfiltrowane na liście).
- Ustal zakres i skutki incydentów: dzięki funkcjom filtrowania nowych lub trwających jakiś czas ataków możesz ustalić ważność wyfiltrowanych incydentów, a także ich wpływ na Twoją firmę.

Po zawężeniu listy do najważniejszych incydentów możesz przeanalizować szczegóły poszczególnych incydentów, aby lepiej poznać ich naturę, a także techniki, których użył atakujący, by osiągnąć swój cel. Aby uzyskać więcej informacji, zobacz "Analizowanie szczegółów incydentu" (s. 969).



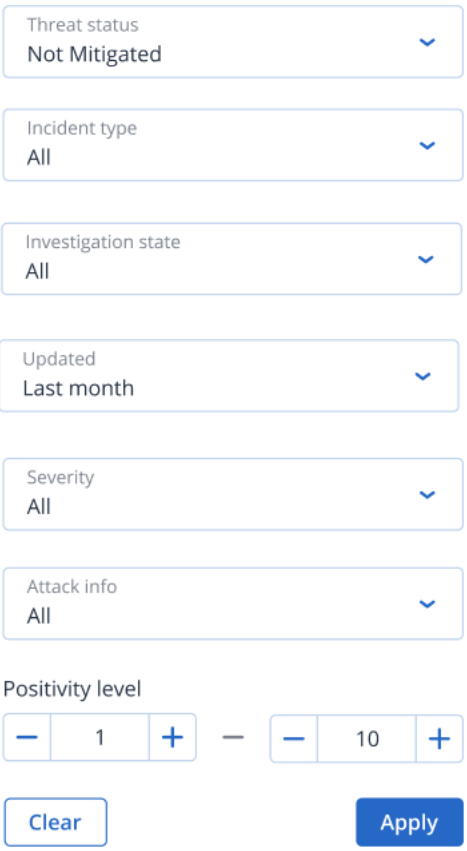
Uwaga
Domyślnie lista incydentów jest posortowana według kolumny **Zaktualizowano**, która zawiera datę i godzinę ostatniej aktualizacji incydentu dokonanej w celu uwzględnienia nowych przypadków wykrycia zjawisk związanych z tym incydentem. Uwaga: każdy już istniejący incydent może w każdej chwili zostać zaktualizowany — nawet jeśli już został zamknięty. W razie potrzeby listę można przefiltrować również tak, aby były na niej wyświetlane nowo otwarte lub trwające jakiś czas ataki — zgodnie z opisem podanym w procedurze poniżej.

Aby przefiltrować listę incydentów

1. U góry listy incydentów kliknij **Filtruj**, aby przefiltrować wyświetlaną listę incydentów. Jeśli na przykład w polu **Utworzono** wybierzesz datę początkową i końcową, na liście incydentów i

© Acronis International GmbH, 2003-2024

widżetach będą wyświetlane incydenty utworzone we wskazanym okresie.



2. Na koniec kliknij **Zastosuj**.

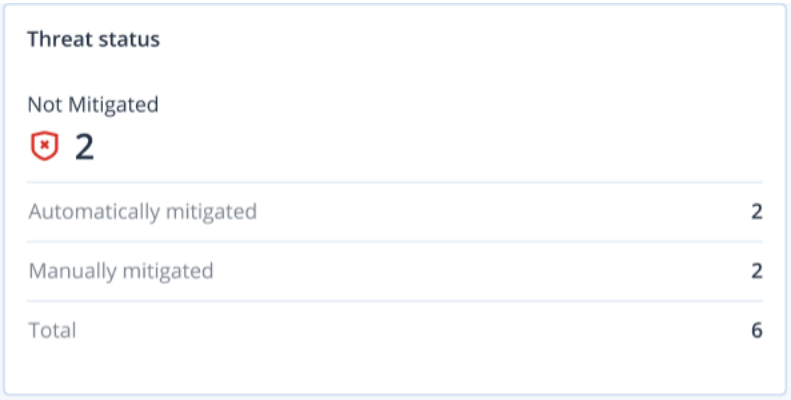
Wyświetlanie incydentów, których skutków jeszcze nie zniwelowano

Bieżące statusy zagrożeń związanych z incydentami można sprawdzić w kolumnie **Status zagrożeń**, w której incydenty są oznaczone jako **Zniwelowano** lub **Nie zniwelowano**. Status zagrożenia jest określany automatycznie przez moduł EDR — każdy incydent, który nie został zniwelowany, powinien zostać jak najszybciej poddany dochodzeniu.

Wyświetloną listę incydentów można dodatkowo zawęzić przez zastosowanie filtrów. Jeśli na przykład zechcesz przefiltrować listę według statusów zagrożeń *oraz* konkretnego poziomu ważności, wybierz odpowiednie opcje filtrowania. Po wyfiltrowaniu interesujących Cię zdarzeń możesz je poddać dochodzeniu zgodnie z opisem podanym w sekcji "Poddawanie incydentów dochodzeniu" (s. 985).

Jak widać na ilustracji poniżej, możesz też użyć widżetu **Status zagrożeń**, aby szybko sprawdzić bieżący status zagrożenia. Uwaga: dane na tym widżecie są wyświetlane z uwzględnieniem zastosowanych filtrów — zobacz sekcję "Aby przefiltrować listę incydentów" (s. 966).

© Acronis International GmbH, 2003-2024



Ustalanie zakresu i skutków incydentów

Wartości kolumn **Ważność**, **Informacje o ataku** oraz **Poziom prawdziwości** pozwalają szybko ustalić zakres i skutki incydentu. Jak już wspomniano, po ustaleniu, które incydenty są obecnie w toku, można filtrować dodatkowe kolumny, aby:

- Sprawdzić, które incydenty są bardziej krytyczne — w kolumnie **Ważność**. Ważność incydentu może zostać oznaczona jako **Krytyczne**, **Wysoki** lub **Średni**.
  - **Krytyczne**: Występuje bardzo duże ryzyko złośliwej aktywności cybernetycznej oraz ryzyko złamania zabezpieczeń krytycznych hostów w danym środowisku.
  - **Wysoki**: Występuje duże ryzyko złośliwej aktywności cybernetycznej oraz ryzyko poważnych szkód w danym środowisku.
  - **Średni**: Występuje podwyższone ryzyko złośliwej działalności cybernetycznej.

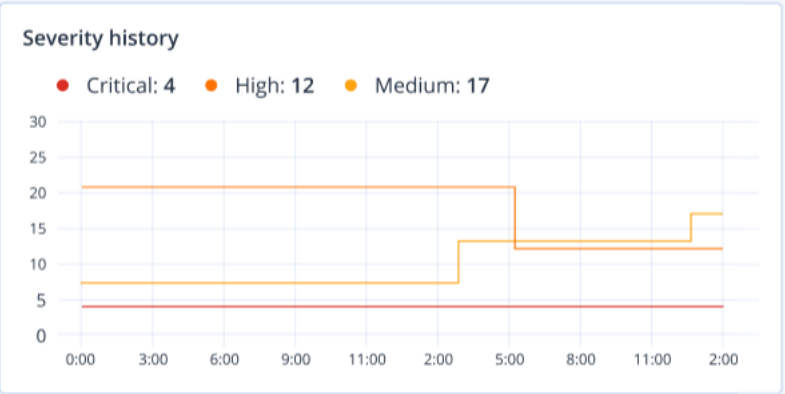
    Uwaga
    W celu ustalenia ważności algorytm modułu EDR uwzględnia typ obciążenia, a także zakres każdego etapu ataku. Jeśli na przykład incydent obejmuje czynności związane z kradzieżą poświadczeń, zostanie oznaczony jako **Krytyczne**.

- W kolumnie **Typ incydentu** sprawdź, dlaczego doszło do incydentu. Może występować jeden lub więcej z poniższych typów incydentów:
  - **Wykryto oprogramowanie ransomware**
  - **Wykryto złośliwe oprogramowanie**
  - **Wykryto podejrzany proces**
  - **Wykryto złośliwy proces**
  - **Zablokowano podejrzany adres URL**
  - **Zablokowano złośliwy adres URL**
- Ustalić, jakimi technikami posłużono się do przeprowadzenia ataku — na podstawie kolumny **Informacje o ataku** — i czy istnieje jakiś wspólny motyw lub wzorzec ataków.
- Sprawdzić prawdopodobieństwo, że dany incydent rzeczywiście jest złośliwym atakiem — kolumna **Poziom prawdziwości** zawiera ocenę w skali od 1 do 10 (im wyższa ocena, tym większe prawdopodobieństwo, że incydent rzeczywiście jest złośliwym atakiem).

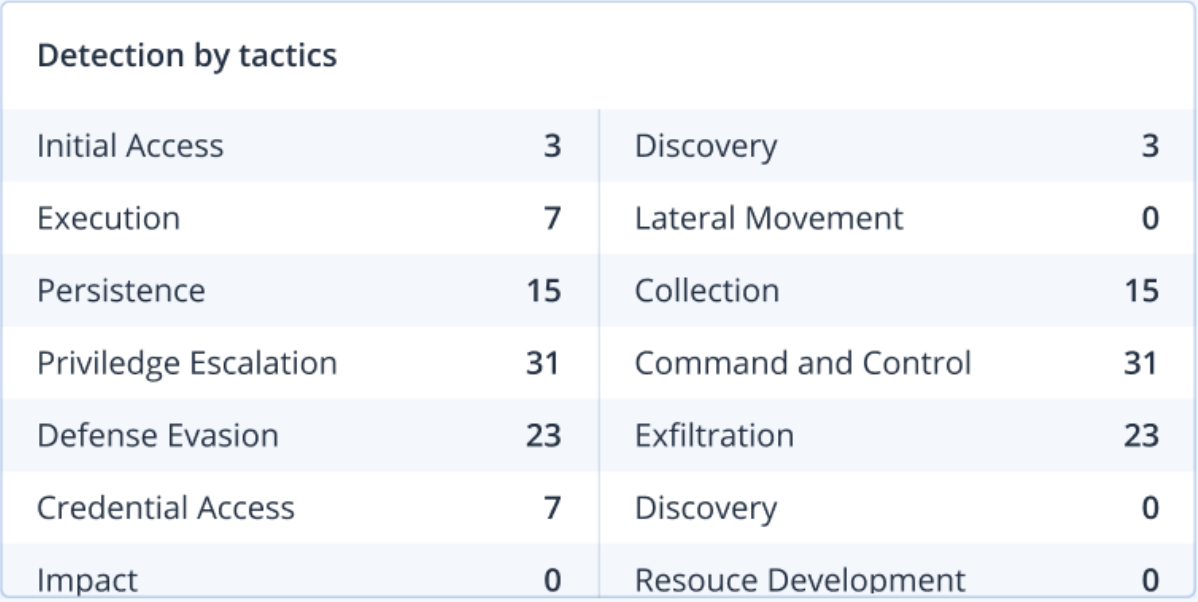
© Acronis International GmbH, 2003-2024

Znalazłszy incydenty wymagające natychmiastowej uwagi, można je poddać dochodzeniu zgodnie z opisem podanym w sekcji "Poddawanie incydentów dochodzeniu" (s. 985).

Można też skorzystać z widżetów **Historia ważności** i **Wykrywanie na podstawie taktyk**, aby szybko uzyskać informacje o ważności i technikach ataków.



Na widżecie **Wykrywanie na podstawie taktyk** wyświetlane są rozmaite używane techniki ataków oraz wartości w kolorze zielonym lub czerwonym wskazujące wzrost lub spadek odnotowany we wskazanym okresie. Widżet ten zapewnia zagregowany obraz wszystkich celów w ramach wyfiltrowanych incydentów, zapewniając szybki obraz ich wpływu na Twoich klientów.



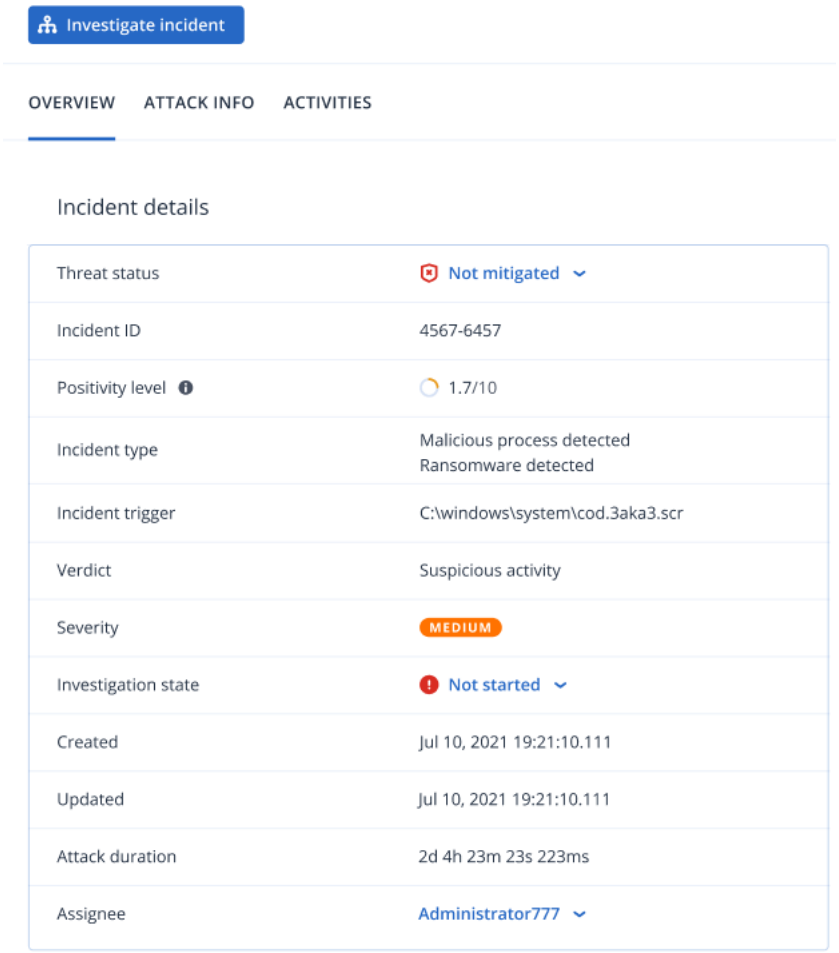
Analizowanie szczegółów incydentu

Na etapie przeglądania incydentu można również analizować szczegóły każdego incydentu z listy incydentów w module Endpoint Detection and Response (EDR). Informacje te pozwalają na głębszy wgląd w cały incydent i ustalenie, jak i kiedy do niego doszło. Ponadto można przypisać incydent do określonych użytkowników w celu przeprowadzenia dochodzenia oraz ustawić status dochodzenia.

Aby przeanalizować szczegóły incydentu

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona > Incydenty**. Zostanie wyświetlona lista incydentów.
2. Kliknij incydent, który chcesz przejrzeć. Zostaną wyświetlone szczegóły wybranego incydentu.
3. Na wyświetlonej karcie **Przegląd** możesz przejrzeć szczegóły incydentu i obciążenia, w tym aktualny status i ważność zagrożenia. Możesz też zdefiniować **Stan dochodzenia** (wybierz **Trwa dochodzenie**, **Nie uruchomiono** (stan domyślny), **Fałszywe zgłoszenie** lub **Zamknięto**) i wybrać użytkownika, do którego ma zostać przypisany incydent (wybierz odpowiedniego użytkownika z listy rozwijanej **Osoba przypisana**).



4. Kliknij kartę **Informacje o ataku**, aby przejrzeć szczegóły ataku i techniki użyte do jego przeprowadzenia. Kliknij łącze widoczne obok wymienionej techniki ataku, aby zapoznać się z dodatkowymi informacjami na jej temat dostępnymi w witrynie internetowej MITRE.org.
5. Kliknij kartę **Działania**, aby przejrzeć wszelkie czynności podjęte w cybernetycznym łańcuchu zabijania w celu zniwelowania skutków incydentu. Aby uzyskać więcej informacji, zobacz "Jak poddać incydenty dochodzeniu w cybernetycznym łańcuchu zabijania" (s. 986).
   Jeśli na przykład na obciążeniu została uruchomiona instalacja poprawki, będzie widać, kto ją zainicjował, ile czasu zajęła i jakie błędy wystąpiły podczas implementacji poprawki.
6. Kliknij **Poddaj incydent dochodzeniu**, aby przejść do cybernetycznego łańcucha zabijania, gdzie możesz poddać incydent dochodzeniu węzeł po węźle. Aby uzyskać więcej informacji, zobacz "Jak poddać incydenty dochodzeniu w cybernetycznym łańcuchu zabijania" (s. 986).

© Acronis International GmbH, 2003-2024

Szukaj wskaźników naruszenia zabezpieczeń (IoC) i podejrzanych działań

Uwaga
Ta funkcja jest dostępna w ramach Programu wczesnego dostępu (PWD). Niektóre funkcje i opisy mogą być niekompletne.

Aby wykryć i zniwelować zagrożenia, zanim przerodzą się w incydenty o poważnym wpływie, użyj funkcji **Wyszukiwanie zdarzeń**. Ta funkcja wyszukiwania umożliwia wyszukiwanie IoC i podejrzanych działań na wszystkich maszynach z włączoną usługą Endpoint Detection and Response (EDR).

Funkcja **Wyszukiwanie zdarzeń** umożliwia:

- Uruchamianie niestandardowych zapytań w odniesieniu do danych zdarzeń zebranych ze wszystkich maszyn w celu wyszukiwania skrótów. Można też uzyskać wskaźniki, aby sobie odpowiedzieć na określone pytania (na przykład wyświetlić maszyny z nadzwyczaj dużą liczbą procesów).
- Filtrowanie zapytań za pomocą atrybutów udostępnionych przez punkty końcowe EDR i danych z innych integracji, takich jak działania systemu operacyjnego, działania użytkowników i działania w sieci.

Dostęp do funkcji **Wyszukiwanie zdarzeń** można uzyskać z menu **Ochrona** w konsoli Cyber Protect.

Uwaga
Domyślny okres przechowywania wyników wyszukiwania zdarzeń EDR wynosi siedem dni.

Wyszukiwanie zdarzeń

Uwaga
Ta funkcja jest dostępna w ramach Programu wczesnego dostępu (PWD). Niektóre funkcje i opisy mogą być niekompletne.

Można wyszukiwać zdarzenia usługi Endpoint Detection and Response (EDR) na wszystkich maszynach chronionych przez EDR.

Pamiętaj, że podczas korzystania z konsoli Cyber Protect na poziomie **(Wszyscy klienci)** dzierżawcy-partnera możesz wyszukiwać zdarzenia od wszystkich zarządzanych klientów. Jeśli pracujesz na poziomie dzierżawcy-klienta, możesz wyszukiwać zdarzenia specyficzne dla wybranego klienta.

Aby wyszukać zdarzenia

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona** > **Wyszukiwanie zdarzeń**.
2. Wprowadź zapytanie wyszukiwania, używając języka zapytań Acronis XDR (XQL) i zdefiniuj zakres dat.

© Acronis International GmbH, 2003-2024

Pamiętaj, że XQL korzysta z autouzupełniania, aby ułatwić tworzenie zapytań. Aby uzyskać więcej informacji na temat dostępnych opcji składni i zapytań, zobacz sekcję "Składnia" (s. 972).

3. Kliknij ikonę strzałki po prawej stronie pola do wprowadzania danych, aby wykonać zapytanie.

   Należy pamiętać, że dostępne są również następujące operacje, które można wykonać przy użyciu klawiatury:

   - Naciśnij klawisz **Enter**, aby przenieść kursor do następnego wiersza. Ponadto na początku nowego wiersza jest dodawany znak „|” (co ułatwia pisanie zapytań wieloetapowych).
   - Naciśnij klawisze **Shift+Enter**, aby przenieść kursor do następnego wiersza.
   - Naciśnij klawisze **Ctrl+Enter**, aby wykonać zapytanie.

4. W razie potrzeby uściślij zapytanie wyszukiwania. Na przykład wybierz wyświetlanie określonych pól lub zdarzeń zawierających określoną nazwę pliku.

Język zapytań Acronis XDR (XQL)

Uwaga
Ta funkcja jest dostępna w ramach Programu wczesnego dostępu (PWD). Niektóre funkcje i opisy mogą być niekompletne.

Języka XQL należy używać do wyszukiwania zdarzeń Endpoint Detection and Response (EDR), a następnie przechodzenia do szczegółów szukanych zdarzeń. W tej sekcji wymieniono różne elementy języka XQL, z którymi należy się zapoznać w przypadku wyszukiwania zdarzeń EDR:

- Składnia (w tym zapytania przykładowe)
- Typy i pola zdarzeń

Więcej informacji na temat korzystania z funkcji **Wyszukiwanie zdarzeń** można znaleźć w sekcji "Szukaj wskaźników naruszenia zabezpieczeń (IoC) i podejrzanych działań" (s. 971).

Składnia

Operacja	Przykład
Wybieranie źródła danych Umożliwia wybranie źródła danych, w odniesieniu do którego ma zostać zastosowane zapytanie. Ten operator musi być pierwszym operatorem w zapytaniu.	`eventType`

Filtrowanie danych
 	
Umożliwia filtrowanie danych na podstawie warunków i musi się zaczynać od słowa kluczowego `where`.
 	
Należy zwrócić uwagę na następujące opcje filtrowania:
 	
• Ciągi znaków można ująć w cudzysłów pojedynczy lub podwójny.
	`eventType | where field == 'value'`
	
	`eventType | where field != 'value'`
	
	`eventType | where field > 'value'`
	
	`eventType | where field < 'value'`
	
	`eventType | where field >= 'value'`

© Acronis International GmbH, 2003-2024

Operacja	Przykład

• Do łączenia filtrów można używać operatorów logicznych, takich jak `AND` czy `OR`.
`key = value AND key < value OR key = value`
• Operatory można ujmować w nawiasy okrągłe:
`(key = value) AND (key < value OR key = value)`
• Operatora `CONTAINS` należy użyć w celu znalezienia częściowo dopasowanego ciągu:
`key CONTAINS 'value'`
• Operatora `ICONTAINS` należy użyć w celu znalezienia częściowo dopasowanego ciągu bez uwzględniania wielkości liter:
`key ICONTAINS 'value'`
• Za pomocą operatora `IN` można sprawdzić przynależność:
`key IN ('value1', 'value2')`
• Dopasowania wyrażeń regularnych należy używać zgodnie ze standardem RE2:
`key MATCHES 'regex string'`
	`eventType | where field <= 'value'`
	`eventType | where field CONTAINS 'substring'`
	`eventType | where field NOT CONTAINS 'substring'`
	`eventType | where field ICONTAINS 'substring'`
	`eventType | where field NOT ICONTAINS 'substring'`
	`eventType | where field IN ('value1', 'value2')`
	`eventType | where field NOT IN ('value1', 'value2')`
	`eventType | where field MATCHES 'value1*'`
	`eventType | where field NOT MATCHES 'value1*'`

Wybieranie pól Określa, które pola mają zostać wybrane i uwzględnione w wynikach zwracanych z zapytania.	`eventType | columns field1, field2, field3 ...`

Sortowanie
Umożliwia sortowanie wyników zapytania — rosnąco lub malejąco. Jeśli nie określono żadnej kolejności, domyślnie jest stosowana kolejność rosnąca.
	`eventType | order field1, field2, field3 ...`
	`eventType | order field asc`
	`eventType | order field desc`

Limit Umożliwia ograniczenie wyników zapytania.	`eventType | limit 10` `eventType | limit 1000 | group [field1, field2] | limit 10`

Operacja grupowa
Umożliwia wykonanie `group operation` na danych.
(Opcjonalnie) Możesz określić funkcje agregujące, które mają być wykonywane na polach zagregowanych, lub określić tylko funkcje agregujące bez wykonywania `group operation` na określonych polach.
	`eventType | group [field]`
	`eventType | group [field1, field2, field3, ...]`
	`eventType | group with [max(field1), min(field2), avg(field3)]`
	`eventType | group [field1, field2, field3, ...] with [max(field1), min (field2), avg(field3)]`

© Acronis International GmbH, 2003-2024

Operacja	Przykład
	`eventType | group [field1, field2, field3, ...] with [max(field1) as max_field, min(field2), avg(field3) as avg_field]`

Agregacja
Umożliwia zagregowanie wyników zapytania w celu wykonania operacji.
Z funkcji tych można korzystać wyłącznie w połączeniu z `group operation` (patrz wyżej).
	`min(field)`
	`max(field)`
	`avg(field)`
	`count()`
	`count(field)`
	`countdistinct(field)`

Przykładowe zapytania

Ta sekcja zawiera kilka przykładowych zapytań ilustrujących sposób stosowania reguł składni XQL w zapytaniu.

- Wybieranie pól z typu zdarzenia `WinProcCreate`:

```
WinProcCreate | fields host_name, parent_start, parent_gpid, parent_pid, parent_
user, proc_name
```

- Filtrowanie przy użyciu warunków przed zgrupowaniem wyników według nazwy procesu (`proc_name`) i zastosowaniem funkcji agregujących `min()` w odniesieniu do `parent_pid`:

```
WinProcCreate | where host_name == 'BNi-Kub' AND parent_pid != -1 AND proc_name
CONTAINS '1' AND host_name IN ('Computer1') | group [proc_name] with [min(parent_
pid)]
```

- Wybieranie danych przy użyciu filtrów, następnie policzenie liczby zwróconych wierszy i uporządkowanie ich w określonej kolejności:

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [count() as new_count] |
order new_count
```


© Acronis International GmbH, 2003-2024

- Wybieranie danych przy użyciu filtrów wyrażeń regularnych:

```
WinProcCreate | where host_name match 'BNi.*'
```

- Wybieranie danych przy użyciu złożonych filtrów i ograniczanie wyników:

```
WinProcCreate | where (host_name contains 'BNi-Kub') OR (host_name in
('Computer1', 'Computer2')) | limit 10
```

- Wybieranie danych przy użyciu filtrów, a następnie policzenie liczby określonych zwróconych wierszy:

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [countdistinct(*)]
```

- Wybieranie danych przy użyciu filtrów, porządkowanie według wybranego pola i ograniczanie liczby zwracanych wierszy:

```
WinProcCreate | where host_name == 'BNi-Kub' | order host_name | limit 10
```

Typy i pola zdarzeń

Ta sekcja zawiera:

- Typy zdarzeń
- Przykładowe typy danych
- Pola zdarzeń

Typy zdarzeń

Nazwa	Opis	Typ
WinProcCreate Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinProcCreate.	Zdarzenia związane z tworzeniem procesów systemu Windows	Wydarzenia
WinProcTerminate	Zdarzenia związane z kończeniem procesów	Wydarzenia

© Acronis International GmbH, 2003-2024

Nazwa	Opis	Typ
Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinProcTerminate.	systemu Windows	
WinNetAccess Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinNetAccess.	Zdarzenia związane z dostępem do sieci systemu Windows	Wydarzenia
WinRegAccess Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinRegAccess.	Zdarzenia związane z dostępem do rejestru systemu Windows	Wydarzenia
WinScriptExec Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinScriptExec.	Zdarzenia związane z wykonywaniem skryptu w systemie Windows (w tym PowerShell, VBS itp.)	Wydarzenia
WinFileAccess Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinFileAccess.	Zdarzenia związane z dostępem do plików systemu Windows (odczyt/zapis)	Wydarzenia
WinLogin Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinLogin.	Zdarzenia związane z logowaniem użytkowników systemu Windows	Wydarzenia
WinLogout Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinLogout.	Zdarzenia związane z wylogowywaniem użytkowników systemu Windows	Wydarzenia
WinAgentDetection Aby uzyskać więcej informacji na temat dostępnych pól, zobacz sekcję WinAgentDetection.	Zdarzenia związane z wykrywaniem w systemie Windows	Wykrycia

Przykładowe typy danych

Typ danych	Przykład	Opis
String	`WinProcCreate | where host_name == 'BNi-Kub'`	Ciągi znaków muszą być ujęte w pojedyncze lub podwójne cudzysłowy.

© Acronis International GmbH, 2003-2024

Typ danych	Przykład	Opis
	`WinProcCreate | where host_name == "BNi-Kub"`	
UUID	`WinProcCreate | where agent_id == '61f0c404-5cb3-11e7-907b-a6006ad3dba0'` `WinProcCreate | where agent_id == "61f0c404-5cb3-11e7-907b-a6006ad3dba0"`	Identyfikatory UUID są ciągami znaków i muszą być ujęte w pojedyncze lub podwójne cudzysłowy. Identyfikatory UUID muszą być podawane w sekwencji 8-4-4-4-12.
DateTime	`WinProcCreate | where event_time < '2022-11-01'` `WinProcCreate | where event_time < "2022-11-01"`	Wartości DateTime są ciągami znaków i muszą być ujęte w pojedyncze lub podwójne cudzysłowy. Wartość DateTime musi mieć format RRRR-MM-DD.

Logiczna	`WinLogin | where is_admin == 1`
	`WinLogin | where is_admin == 0`
	`WinLogin | where is_admin == true`
	`WinLogin | where is_admin == false`
		Wartości logiczne mogą być reprezentowane przez `1`, `0`, `true` lub `false`.

Liczba całkowita	`WinLogin | where proc_pid > 25`	Wartość jest liczbą całkowitą.

Pola zdarzeń

Typ zdarzenia	Pole (typ danych)
WinProcCreate	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String)

© Acronis International GmbH, 2003-2024

Typ zdarzenia	Pole (typ danych)
	• parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_prod (String) • proc_prod_desc (String) • proc_sha1 (String) • proc_sha256 (String) • proc_signatures (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinProcTerminate	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String)

© Acronis International GmbH, 2003-2024

Typ zdarzenia	Pole (typ danych)
	• proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • term_args (String) • term_gpid (UUID) • term_integrity_level (String) • term_md5 (String) • term_name (String) • term_oname (String) • term_path (String) • term_pid (Int) • term_sha1 (String) • term_sha256 (String) • term_start (DateTime) • term_upn (String) • term_user (String) • term_user_domain (String) • timestamp (DateTime)
WinNetAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • net_dst_ip (String) • net_dst_port (Int) • net_host (String) • net_http_method (String) • net_http_url (String) • net_protocol (String) • net_src_ip (String) • net_src_port (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String)

© Acronis International GmbH, 2003-2024

Typ zdarzenia	Pole (typ danych)
	• parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinRegAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String)

© Acronis International GmbH, 2003-2024

Typ zdarzenia	Pole (typ danych)
	• parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • reg_key (String) • reg_operation (String) • reg_original_key (String) • reg_original_value_data (String) • reg_value_data (String) • reg_value_name (String) • reg_value_type (String) • resource_id (UUID) • timestamp (DateTime)
WinScriptExec	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String)

© Acronis International GmbH, 2003-2024

Typ zdarzenia	Pole (typ danych)
	• parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • script_data (String) • script_fragment (Bool) • script_size (Int) • script_type (String) • timestamp (DateTime)
WinFileAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_op (String) • file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • owner (String) • parent_args (String)

© Acronis International GmbH, 2003-2024

Typ zdarzenia	Pole (typ danych)
	• parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinLogin	• agent_id (UUID) • customer (String) • domain (String) • event_time (DateTime) • host_name (String) • id (UUID) • is_admin (Bool) • login_time (DateTime) • name (String) • owner (String) • resource_id (UUID)

© Acronis International GmbH, 2003-2024

Typ zdarzenia	Pole (typ danych)
	• security_id (String) • timestamp (DateTime) • type (String)
WinLogout	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • logout_time (DateTime) • resource_id (UUID) • security_id (String) • timestamp (DateTime)
WinAgentDetection	• agent_id (UUID) • customer (String) • detection_type (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • mitre_stid (Int) • mitre_tactics (Array(Int)) • mitre_tid (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String)

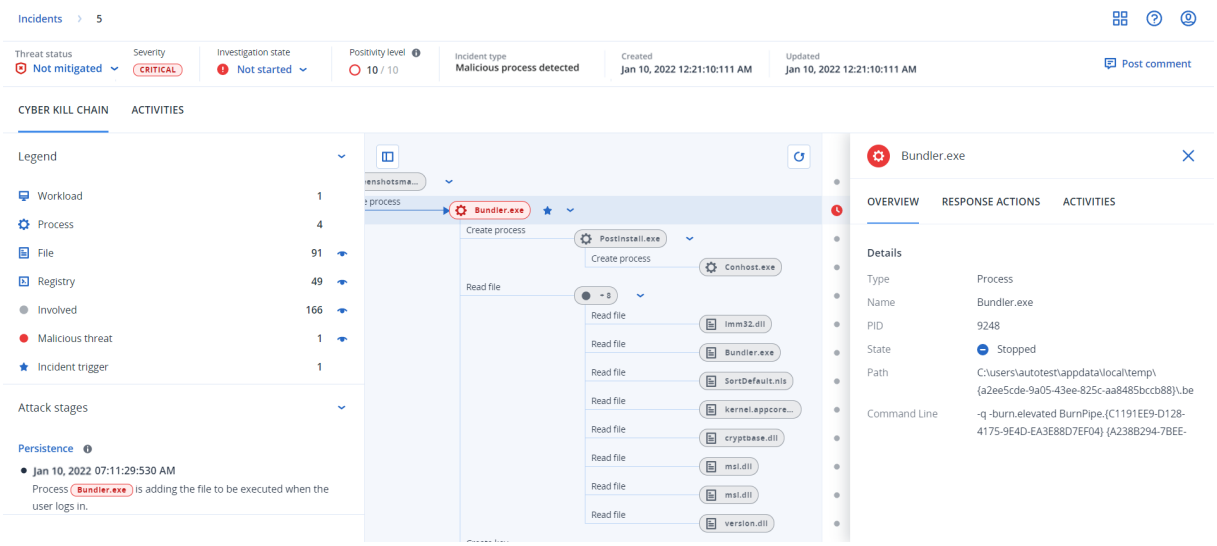
© Acronis International GmbH, 2003-2024

Typ zdarzenia	Pole (typ danych)
	• parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • severity (String) • threat_name (String) • timestamp (DateTime) • url (String) • url_blocked (Bool) • url_cat (Array(String)) • url_list (String) • url_md5 (String)

Poddawanie incydentów dochodzeniu

Moduł Endpoint Detection and Response (EDR) umożliwia prowadzenie dochodzeń obejmujących cały incydent, w tym wszystkie etapy ataku i obiekty (procesy, rejestry, zaplanowane zadania i domeny), które ucierpiały wskutek ataku. Obiekty te są reprezentowane przez węzły w przejrzyście przedstawionym cybernetycznym łańcuchu zabijania, jak widać poniżej. Dzięki cybernetycznemu łańcuchowi zabijania można szybko ustalić, co dokładnie się stało i kiedy.

© Acronis International GmbH, 2003-2024



Każdy etap ataku jest widoczny w cybernetycznym łańcuchu, który udostępnia szczegółową interpretację tego, jak i dlaczego doszło do incydentu. Cybernetyczny łańcuch zabijania obejmuje przystępnie sformułowane zdania i przejrzyste wykresy, które ułatwiają wyjaśnienie każdego etapu ataku, a to z kolei przekłada się na minimalny czas trwania dochodzenia.

Z kolei zamapowanie ewolucji ataku na strukturę MITRE umożliwia szybkie ustalenie zakresu i skutków incydentu. Pozwala to przeanalizować, co się działo na każdym etapie ataku, i odkryć między innymi:

- Punkt przedostania się ataku do środowiska
- Sposób przeprowadzenia ataku
- Ewentualne eskalacje uprawnień
- Metody ukrycia ataku przed technikami wykrywania
- Przenoszenie się ataku na inne obciążenia
- Kradzież poświadczeń
- Próby eksfiltracji

Uwaga

Każdy obiekt objęty atakiem — bez względu na to, czy chodzi o proces, rejestr, zaplanowane zadanie czy domenę — jest reprezentowany w cybernetycznym łańcuchu zabijania za pomocą węzła.

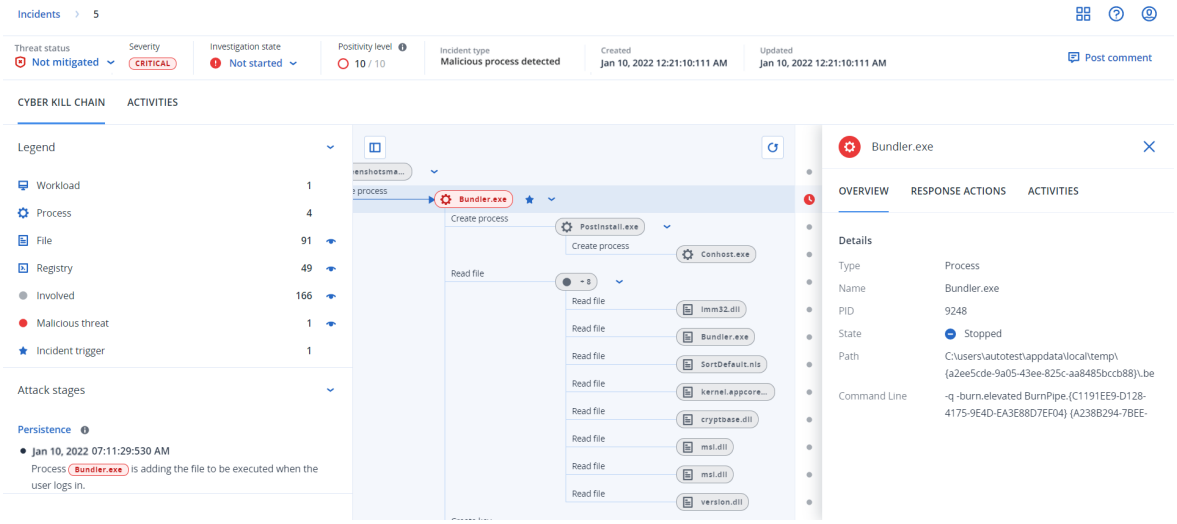
Jak poddać incydenty dochodzeniu w cybernetycznym łańcuchu zabijania

Każdy etap ataku w cybernetycznym łańcuchu zabijania można poddać dochodzeniu. Postępuj zgodnie z przystępnie sformułowanymi zdaniami i wykresami dostępnymi w ramach cybernetycznego łańcucha zabijania, aby dobrze poznać każdy etap ataku, co z kolei przełoży się na minimalny czas trwania dochodzenia.

Aby rozpocząć dochodzenie w cybernetycznym łańcuchu zabijania

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona > Incydenty**.
2. Na wyświetlonej liście incydentów kliknij w pierwszej kolumnie z prawej strony w obszarze incydentu, który chcesz poddać dochodzeniu. Zostanie wyświetlony cybernetyczny łańcuch zabijania dotyczący wybranego incydentu.



3. Sprawdź podsumowanie incydentu na pasku statusu zagrożenia u góry strony. Pasek statusu zagrożenia zawiera następujące informacje:
   - Bieżący status zagrożenia: jest on określany automatycznie przez system. Incydent o statusie **Nie zniwelowano** należy jak najszybciej poddać dochodzeniu.

     Ważne
     Status incydentu zostanie ustawiony jako **Zniwelowano** po pomyślnym ukończeniu przywracania z kopii zapasowej lub naprawieniu wszystkich wykryć przez zatrzymanie procesu, kwarantannę lub wycofanie.

     Status incydentu zostanie ustawiony jako **Nie zniwelowano**, jeśli nie uda się pomyślnie ukończyć przywracania z kopii zapasowej lub choć jedno wykrycie nie zostanie pomyślnie naprawione przez zatrzymanie procesu, kwarantannę lub wycofanie.

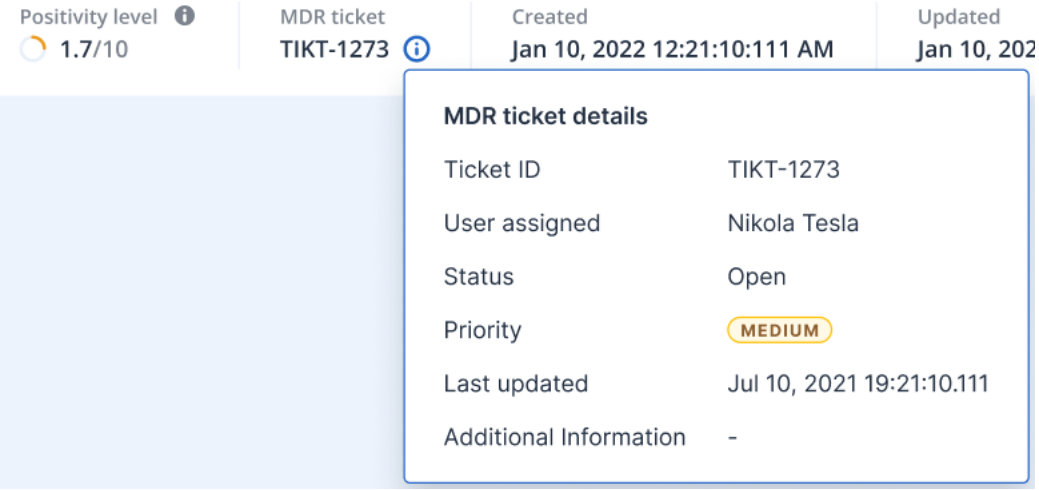
     Można też ręcznie ustawić status zagrożenia **Zniwelowano** lub **Nie zniwelowano**. Po wybraniu jednego z tych statusów zostanie wyświetlony monit o wprowadzenie komentarza. Komentarz ten zostanie zapisany jako część działań dochodzeniowych i można go wyświetlić na karcie **Działania**. Należy pamiętać, że EDR wciąż może przywrócić stan zagrożenia **Zniwelowano** lub **Nie zniwelowano** w przypadku nowego wykrycia incydentu lub uruchomienia i pomyślnego wykonania czynności w ramach reagowania.

   - Ważność incydentu: **Krytyczne**, **Wysoki** lub **Średni**. Aby uzyskać więcej informacji, zobacz "Przeglądanie incydentów" (s. 964).
   - Bieżący stan dochodzenia: **Trwa dochodzenie**, **Nie uruchomiono** (stan domyślny), **Fałszywe zgłoszenie** lub **Zamknięto**. Po rozpoczęciu dochodzenia w sprawie incydentu warto zmienić

© Acronis International GmbH, 2003-2024

jego stan, tak aby inni współpracownicy wiedzieli o wszelkich zmianach związanych z incydentem.

- Stopień pewności: wskazuje stopień prawdopodobieństwa, że dany incydent rzeczywiście jest złośliwym atakiem — w skali od 1 do 10. Aby uzyskać więcej informacji, zobacz "Przeglądanie incydentów" (s. 964).
- Typ incydentu — co najmniej jeden z następujących: **Wykryto oprogramowanie ransomware**, **Wykryto złośliwe oprogramowanie**, **Wykryto podejrzany proces**, **Wykryto złośliwy proces**, **Zablokowano podejrzany adres URL** i **Zablokowano złośliwy adres URL**.
- Jeśli na maszynie jest włączona usługa Zarządzane wykrywanie i reagowanie ((Managed Detection and Response, MDR), jest wyświetlane pole **Zgłoszenie usługi MDR**. Możesz wyświetlić szczegóły zgłoszenia usługi MDR utworzonego w przypadku danego incydentu oraz analityka ds. ochrony MDR przypisanego do danego incydentu.



- Kiedy incydent został utworzony i zaktualizowany: data i godzina wykrycia incydentu lub data ostatniej aktualizacji incydentu z uwzględnieniem nowych wykryć zarejestrowane w ramach tego incydentu.

4. Kliknij kartę **Legenda**, aby wyświetlić różne węzły składające się na wykres łańcucha zabijania i wskazać, które węzły mają być wyświetlane. Dodatkowe informacje można znaleźć w sekcji "Zapoznawanie się z widokiem cybernetycznego łańcucha zabijania i jego dostosowywanie" (s. 989).
5. Poddaj incydent dochodzeniu i go napraw, podejmując następujące kroki. Należy pamiętać, że jest to typowy przepływ pracy związany z dochodzeniem i naprawą incydentu, ale może on wyglądać inaczej, w zależności od incydentu i własnych wymagań.
   a. Poddaj dochodzeniu każdy etap ataku widoczny na karcie **Etapy ataku**. Dodatkowe informacje można znaleźć w sekcji "Jak się poruszać po etapach ataku" (s. 991).
   b. Kliknij **Napraw cały incydent**, aby zastosować czynności naprawcze. Dodatkowe informacje można znaleźć w sekcji "Naprawianie całego incydentu" (s. 1002).

      Możesz też stosować czynności naprawcze w odniesieniu do pojedynczych węzłów z cybernetycznego łańcucha zabijania — zgodnie z opisem podanym w sekcji "Czynności w

© Acronis International GmbH, 2003-2024

ramach reagowania dotyczące indywidualnych węzłów z cybernetycznego łańcucha zabijania" (s. 1007).

c. Na karcie **Działania** przejrzyj czynności podjęte w celu zniwelowania skutków incydentu. Dodatkowe informacje można znaleźć w sekcji "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Zapoznawanie się z widokiem cybernetycznego łańcucha zabijania i jego dostosowywanie

Aby się dowiedzieć, jakich węzłów dotyczy cybernetyczny łańcuch zabijania, zajrzyj do legendy. W obszarze legendy wyświetlane są wszystkie węzły mające związek z incydentem, dzięki czemu można ustalić, jaki wpływ wywarł incydent na poszczególne węzły. Można też wskazać, które węzły mają być ukryte lub wyświetlane w cybernetycznym łańcuchu zabijania.

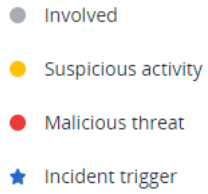
Aby otworzyć legendę

1. Kliknij ikonę strzałki widoczną po prawej stronie sekcji Legenda.
   Sekcja Legenda zostanie rozwinięta, jak pokazano na poniższej ilustracji.

2. W legendzie zastosowano cztery główne kolory, które pozwalają szybko ustalić, co się stało z poszczególnymi węzłami w cybernetycznym łańcuchu zabijania, jak pokazano na poniższej ilustracji. Te oznaczone kolorami węzły są też uwzględniane w etapach ataku, jak opisano w

© Acronis International GmbH, 2003-2024

sekcji "Jak się poruszać po etapach ataku" (s. 991).



Aby ukryć lub wyświetlić węzły w cybernetycznym łańcuchu zabijania

1. W rozwiniętej sekcji Legenda dopilnuj, aby obok węzłów, które mają być wyświetlane w cybernetycznym łańcuchu zabijania, była wyświetlana ikona . Jeśli jest wyświetlana ikona , kliknij ją, aby została zmieniona w ikonę .
2. Aby ukryć węzeł w cybernetycznym łańcuchu zabijania, kliknij . Ikona zostanie zmieniona w ikonę , a węzeł nie będzie wyświetlany w cybernetycznym łańcuchu zabijania.

Przeprowadzanie dochodzenia dotyczącego etapów ataku w ramach incydentu

Etapy ataku w ramach incydentu udostępniają przystępne interpretacje incydentu.

Każdy etap ataku zawiera podsumowanie, co się dokładnie stało i jakie obiekty (nazywane *węzłami* w cybernetycznym łańcuchu zabijania) obrano za cel. Jeśli na przykład pobrany plik zostanie fałszywie zaprezentowany jako coś innego, w ramach etapu ataku problem ten będzie zasygnalizowany i zostaną udostępnione łącza do odpowiedniego węzła w cybernetycznym łańcuchu zabijania, który można poddać dochodzeniu, oraz do odpowiedniej techniki MITRE ATT&CK.

Każdy etap ataku udostępnia informacje potrzebne do znalezienia odpowiedzi na trzy kluczowe pytania:

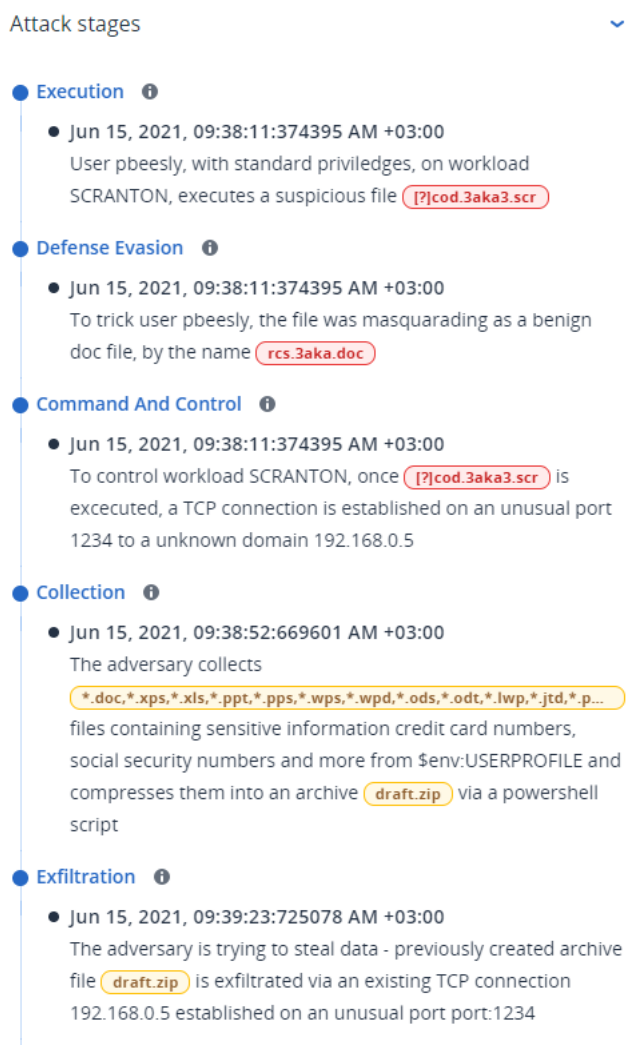
- Jaki haker miał cel?
- Jak haker ten cel osiągnął?
- Na które węzły przypuszczono atak?

Co ważniejsze, udostępniona interpretacja znacznie skraca czas poświęcany na dochodzenie w sprawie incydentu, ponieważ eliminuje konieczność analiz każdego zdarzenia związanego z bezpieczeństwem na osi czasu lub wykresie węzła, a następnie prób interpretacji ataku.

Etapy ataku zawierają również informacje o plikach zawierających informacje wrażliwe — takie jak numery kart kredytowych czy numery ubezpieczenia społecznego — których zabezpieczenia złamano, jak widać w etapie **Zbieranie** w poniższym przykładzie.

Aby uzyskać więcej informacji, zobacz "Jakie informacje są dostępne w ramach etapu ataku?" (s. 991).

© Acronis International GmbH, 2003-2024



Jak się poruszać po etapach ataku

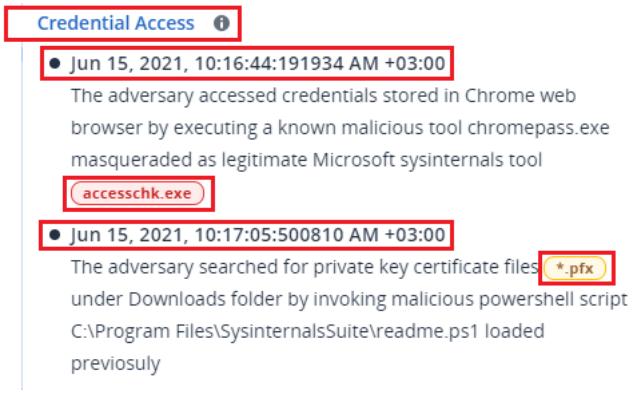
Etapy ataku są ułożone w kolejności chronologicznej. Przewiń w dół, aby wyświetlić pełną listę etapów ataku w ramach incydentu.

Aby przeprowadzić dokładniejsze dochodzenie w przypadku określonego etapu ataku, kliknij dowolne miejsce w etapie ataku, aby przejść do odpowiedniego węzła na wykresie cybernetycznego łańcucha zabijania. Dodatkowe informacje na temat poruszania się po wykresie cybernetycznego łańcucha zabijania i poszczególnych węzłach można znaleźć w sekcji "Poddawanie dochodzeniu pojedynczych węzłów z cybernetycznego łańcucha zabijania" (s. 993).

Jakie informacje są dostępne w ramach etapu ataku?

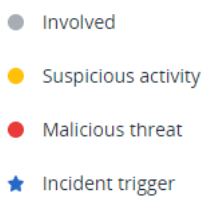
Każdy etap ataku udostępnia przystępną interpretację ataku, napisaną łatwo zrozumiałym dla człowieka językiem. Interpretacja ta składa się z różnych elementów, zestawionych i opisanych w poniższej tabeli.

© Acronis International GmbH, 2003-2024



Element etapu ataku	Opis
Nagłówek	Jest to opis, co próbował zrobić atakujący oraz jaki był jego cel (w powyższym przykładzie: **Dostęp przy użyciu poświadczeń**), a także łącze do znanej techniki MITRE ATT&CK. Kliknij to łącze, aby się zapoznać z dodatkowymi informacjami dostępnymi w witrynie internetowej MITRE ATT&CK. **Uwaga** Jeśli etap ataku nie jest znaną techniką MITRE ATT&CK, tekst nagłówka nie będzie sformatowany jako łącze. Dotyczy to powszechnie stosowanych technik, takich jak pliki wykryte w losowym folderze.
Sygnatura czasowa	Czas wystąpienia danego etapu ataku.
Technika	Jak atakujący osiągnął swój cel z technicznego punktu widzenia i które obiekty (wpisy rejestru, pliki lub zaplanowane zadania) ucierpiały wskutek jego działań. W tekstowym opisie techniki ataku znajdują się oznaczone kolorem łącza do każdego dotkniętego problemem węzła w cybernetycznym łańcuchu zabijania, jak widać w powyższym przykładzie. Te oznaczone kolorami łącza umożliwiają szybkie przechodzenie do dotkniętego problemem węzła i przeprowadzenie dochodzenia, co dokładnie się stało. Oto znaczenia kolorów używanych w ramach etapu ataku:

© Acronis International GmbH, 2003-2024

Element etapu ataku	Opis
	 Na powyższej legendzie widać, że przykładowy etap ataku typu Dostęp przy użyciu poświadczeń zawiera łącze do węzła złośliwego oprogramowania accesschk.exe oraz węzła podejrzanego pliku *.pfx (wystarczy je kliknąć, aby przejść do odpowiedniego węzła w cybernetycznym łańcuchu zabijania). Więcej informacji na temat poruszania się po tych węzłach i dostępnych czynności można znaleźć w sekcji "Poddawanie dochodzeniu pojedynczych węzłów z cybernetycznego łańcucha zabijania" (s. 993). Uwaga: etapy ataku zawierają również łącza do węzłów plików z informacjami o plikach zawierających informacje wrażliwe — takie jak chronione informacje dotyczące zdrowia (PHI), numery kart kredytowych czy numery ubezpieczenia społecznego — których zabezpieczenia złamano.

Uwaga
Każdy etap ataku stanowi jedno zdarzenie wykrycia. Zawartość wymieniona w każdym etapie (nagłówek, sygnatura czasowa, technika) jest generowana zgodnie z określonymi parametrami w zdarzeniu wykrycia i oparta na szablonach etapów ataków przechowywanych przez moduł Endpoint Detection and Response (EDR).

Poddawanie dochodzeniu pojedynczych węzłów z cybernetycznego łańcucha zabijania

Oprócz przeglądania etapów ataków, masz też możliwość poruszania się po poszczególnych węzłach ataku w ramach cybernetycznego łańcucha zabijania. Umożliwia to przechodzenie do konkretnych węzłów w cybernetycznym łańcuchu zabijania oraz poddawanie ich dochodzeniu i naprawianie każdego z nich stosownie do potrzeb.

Można na przykład ustalić stopień prawdopodobieństwa, że dany incydent rzeczywiście jest złośliwym atakiem. Na podstawie przeprowadzonego dochodzenia można też zastosować do węzła szereg czynności w ramach reagowania, między innymi odizolować obciążenie lub poddać podejrzany plik kwarantannie.

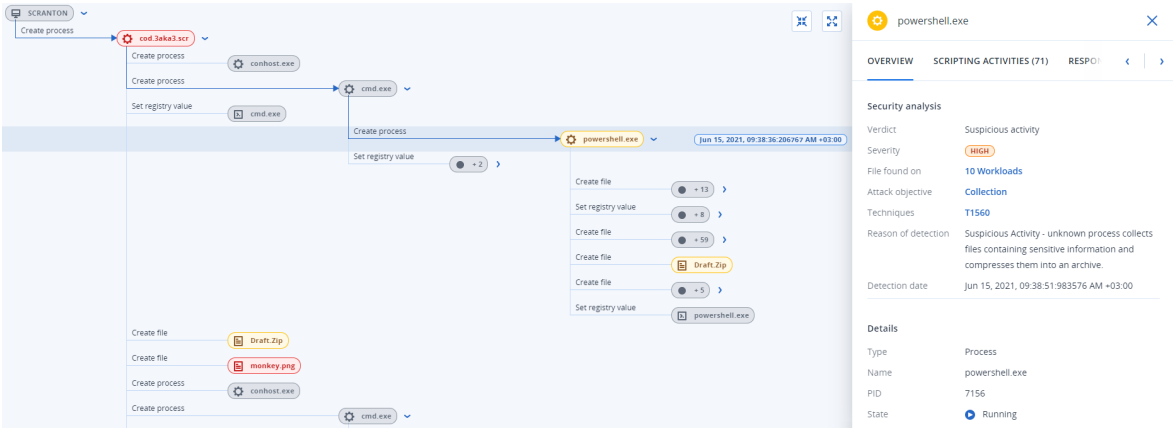
© Acronis International GmbH, 2003-2024

Aby poddać dochodzeniu pojedyncze węzły z cybernetycznego łańcucha zabijania

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona > Incydenty**.
2. Na wyświetlonej liście incydentów kliknij w pierwszej kolumnie z prawej strony w obszarze incydentu, który chcesz poddać dochodzeniu. Zostanie wyświetlony cybernetyczny łańcuch zabijania dotyczący wybranego incydentu.
3. Przejdź do odpowiedniego węzła i go kliknij, aby wyświetlić odpowiadający mu pasek boczny.

Uwaga
Kliknij węzeł, aby go rozwinąć i wyświetlić węzły, które są z nim powiązane.

Na przykład kliknięcie węzła **powershell.exe** w poniższym przykładzie spowoduje otwarcie paska bocznego dla tego węzła. Możesz też kliknąć ikonę strzałki obok węzła, aby wyświetlić powiązane z nim węzły, w tym pliki i wartości rejestru, na które mógł wywrzeć wpływ węzeł **powershell.exe**. Potem możesz klikać te powiązane węzły, aby je poddać dokładniejszemu dochodzeniu.



4. Przeprowadź dochodzenie na podstawie informacji zawartych na kartach paska bocznego:
   - **Przegląd**: Obejmuje dwie główne sekcje, które zawierają podsumowanie poziomu ochrony zaatakowanego węzła.
     - **Analiza zabezpieczeń**: Przedstawia analizę zaatakowanego węzła, w tym werdykt EDR dotyczący zagrożenia (na przykład podejrzane działanie), cel ataku według technik MITRE (kliknij łącze, aby przejść do witryny internetowej MITRE), przyczynę wykrycia oraz liczbę obciążeń, których może dotyczyć atak (kliknij łącze **n obciążeń**, aby wyświetlić obciążenia, których dotyczy problem).

Uwaga
Łącze **n obciążeń** oznacza, że dany złośliwy lub podejrzany obiekt *znaleziono* na innych obciążeniach. Nie oznacza to, że atak jest przeprowadzany na tych innych obciążeniach, tylko że na tych innych obciążeniach występuje wskaźnik naruszenia zabezpieczeń. Być może atak już został przeprowadzony (i spowodował utworzenie kolejnego incydentu), a być może haker dopiero przygotowuje się do ataku na te inne obciążenia przy użyciu swojego „zestawu narzędzi” do ataku.

© Acronis International GmbH, 2003-2024

- **Szczegóły**: Zawiera szczegóły dotyczące węzła, w tym jego typ, nazwę i bieżący stan, ścieżkę do węzła oraz wszelkie skróty plików i podpisy cyfrowe (np. skróty MD5 i numery seryjne certyfikatów).

- **Działania dotyczące skryptów**: Zawiera szczegółowe informacje o wszelkich skryptach wywoływanych lub ładowanych w ramach ataku. Kliknij , aby skopiować skrypt do schowka w celu poddania go dokładniejszemu dochodzeniu.

  Uwaga
  Karta **Działania dotyczące skryptów** jest wyświetlana tylko w przypadku węzłów procesów, które uruchamiają polecenia lub skrypty (na przykład cmd lub PowerShell).

- **Czynności w ramach reagowania**: Zawiera sekcje, które udostępniają dodatkowe czynności dochodzeniowe, naprawcze i zapobiegawcze, w zależności od typu węzła. Zawiera sekcje, które udostępniają dodatkowe czynności dochodzeniowe, naprawcze i zapobiegawcze, w zależności od typu węzła.
  Na przykład w przypadku węzłów obciążeń można zdefiniować szereg czynności, między innymi utworzenie kopii zapasowej na potrzeby analizy śledczej oraz przywrócenie z kopii zapasowej. W przypadku złośliwych lub podejrzanych węzłów można zatrzymać węzeł lub poddać go kwarantannie, cofnąć zmiany wprowadzone przez atak i dodać węzeł do listy dozwolonych lub listy zablokowanych w planie ochrony.
  Dodatkowe informacje na temat wykonywania czynności w ramach reagowania w odniesieniu do konkretnych węzłów można znaleźć w sekcji "Czynności w ramach reagowania dotyczące indywidualnych węzłów z cybernetycznego łańcucha zabijania" (s. 1007).
- **Działania**: Umożliwia wyświetlenie czynności zastosowanych do incydentu w kolejności chronologicznej. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Poznawanie czynności podjętych w celu zniwelowania skutków incydentu

Po przejrzeniu incydentu i przeprowadzeniu dochodzenia w celu ustalenia przebiegu ataku zwykle są stosowane czynności w ramach reagowania. Po zastosowaniu czynności w ramach reagowania można je przeglądać w kilku miejscach, aby dokładniej się dowiedzieć, jakie kroki zostały podjęte w celu zniwelowania skutków incydentu.

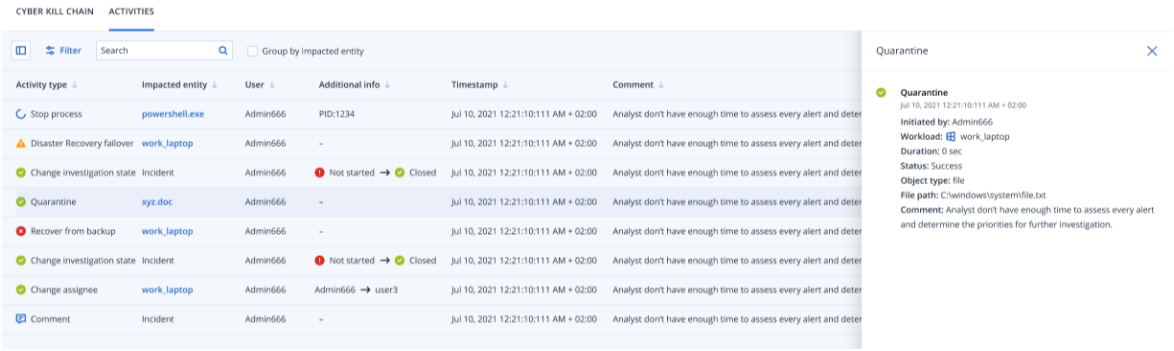
Uwaga
W odniesieniu do incydentów tworzonych przez warstwy zapobiegawcze automatycznie są stosowane czynności skonfigurowane w planie ochrony. W przypadku punktów wykrywania trzeba zdefiniować odpowiednie czynności w ramach reagowania, aby zniwelować skutki w każdym scenariuszu ataku.

Aby sprawdzić podjęte czynności w ramach reagowania, można wyświetlić czynności zastosowane do całego incydentu lub czynności zastosowane do określonego węzła w cybernetycznym łańcuchu zabijania dotyczącym danego incydentu.

© Acronis International GmbH, 2003-2024

Aby wyświetlić wszystkie czynności w ramach reagowania zastosowane w odniesieniu do incydentu

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona > Incydenty**.
2. Na wyświetlonej liście incydentów kliknij w pierwszej kolumnie z prawej strony w obszarze incydentu, który chcesz poddać dochodzeniu. Zostanie wyświetlony cybernetyczny łańcuch zabijania dotyczący wybranego incydentu.
3. Kliknij kartę **Działania**.
   Zostanie wyświetlona lista czynności w ramach reagowania, które już zostały zastosowane w odniesieniu do incydentu.



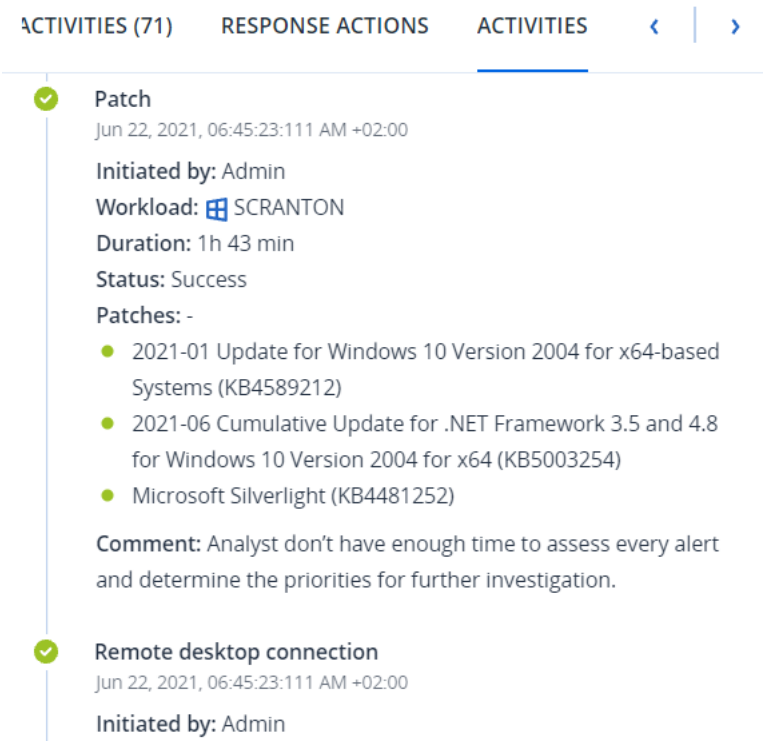
4. Na wyświetlonej liście można wykonać szereg czynności:
   - Kliknij wiersz typu działania, aby wyświetlić więcej informacji na temat wybranego działania. Informacje zostaną wyświetlone na pasku bocznym, jak pokazano w kroku 3, i będą obejmowały informacje o osobie inicjującej czynność, status czynności, ścieżkę pliku i wszelkie komentarze dodane przez inicjatora.
   - Skorzystaj z pola **Szukaj**, aby wyszukać określoną czynność.
   - Kliknij **Filtruj**, aby zastosować filtry do listy.
   - Zaznacz pole wyboru **Grupuj według jednostek dotkniętych problemem**, aby pogrupować odpowiednie czynności według jednostek.
   - Kliknij ikonę , aby wyświetlić lub ukryć listę ukończonych czynności.
     Dopilnuj, aby obok czynności, które mają być wyświetlane, była wyświetlana ikona . Jeśli chcesz ukryć czynność na wyświetlanej liście, ponownie kliknij tę ikonę, aby została zmieniona w ikonę .

© Acronis International GmbH, 2003-2024

Aby wyświetlić czynności w ramach reagowania zastosowane w odniesieniu do konkretnego węzła

© Acronis International GmbH, 2003-2024

1. W cybernetycznym łańcuchu zabijania kliknij wybrany węzeł, aby wyświetlić jego pasek boczny.
2. Kliknij kartę **Działania**.



3. Aby uzyskać pełne informacje o tym, jakie czynności zostały zastosowane i dlaczego, może być konieczne przewinięcie czynności w ramach reagowania zastosowanych w odniesieniu do danego węzła. Na przykład w przypadku czynności podejmowanych w ramach połączenia pulpitu zdalnego będzie widać, kto i kiedy rozpoczął czynność, jak długo trwało jej wykonywanie i jaki jest jej status ogólny (czy zakończyła się sukcesem, niepowodzeniem lub błędami).

Sprawdzanie obciążeń pod kątem występowania wskaźników naruszenia zabezpieczeń (IOC) z publicznie znanych ataków

Moduł Endpoint Detection and Response (EDR) umożliwia między innymi przeglądanie obciążeń pod kątem już gdzieś przeprowadzonych, znanych ataków, które udokumentowano w kanałach dotyczących zagrożeń. Kanały dotyczące zagrożeń są generowane automatycznie na podstawie danych o zagrożeniach pozyskiwanych z Cyber Protection Operations Center (CPOC). Moduł EDR umożliwia sprawdzenie, czy takie zagrożenie wywarło negatywny wpływ na obciążenie, a następnie podjęcie niezbędnych kroków w celu wyeliminowania zagrożenia.

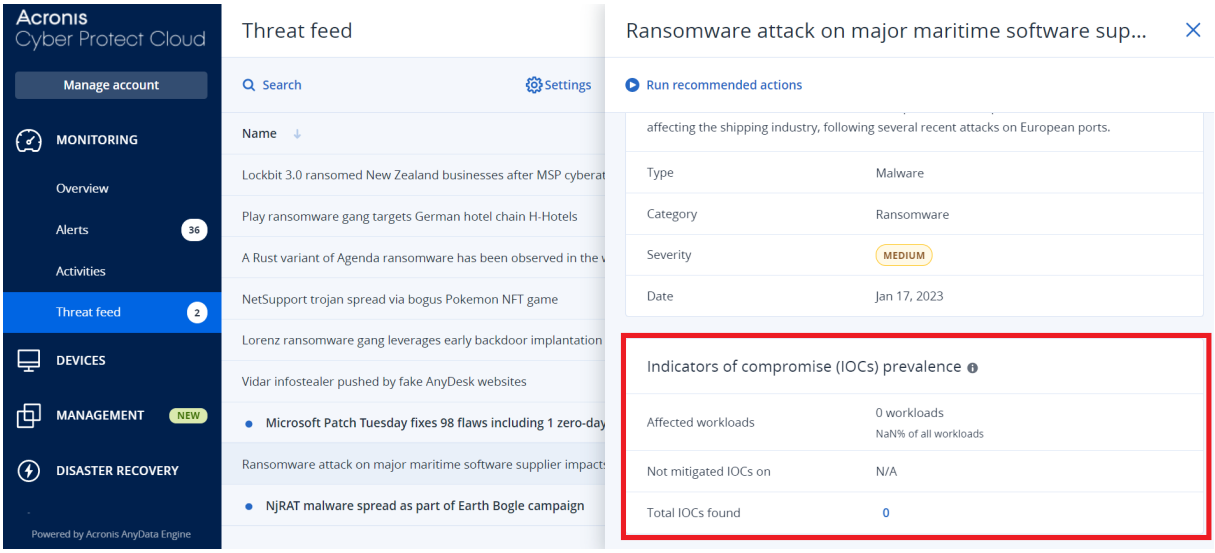
Dostęp do kanałów dotyczących zagrożeń można uzyskać z menu **Monitorowanie** w konsoli Cyber Protect. Aby uzyskać więcej informacji, zobacz "Kanał dotyczący zagrożeń" (s. 297).

Aby przejrzeć szczegółowe informacje o konkretnych zagrożeniach i sprawdzić, czy wywarły one wpływ na Twoje obciążenia, kliknij kanał dotyczący zagrożeń. Możesz wyświetlić liczbę wykrytych wskaźników IOC i obciążeń, na których one wystąpiły, a także przejść do obciążeń zawierających niezniwelowane wskaźniki IOC.

© Acronis International GmbH, 2003-2024

Uwaga

Jeśli w planie ochrony nie włączono modułu EDR, ta dodatkowa funkcja kanałów dotyczących zagrożeń, jak pokazano na poniższej ilustracji, nie jest wyświetlana.



Określanie ustawień kanałów dotyczących zagrożeń

Można określić pewne ustawienia kanału dotyczącego zagrożeń, aby automatycznie lokalizować ewentualne znane zagrożenia i niwelować ich skutki.

Aby określić ustawienia kanałów dotyczących zagrożeń

1. W konsoli Cyber Protect przejdź do sekcji **Monitorowanie > Kanał dotyczący zagrożeń**.
2. Na wyświetlonej stronie Kanał dotyczący zagrożeń kliknij **Ustawienia**.

© Acronis International GmbH, 2003-2024

3. W wyświetlonym oknie dialogowym wybierz dowolne z następujących opcji:

Opcja	Opis
Szukaj wskaźników naruszenia zabezpieczeń (IOC)	Kliknij ten przełącznik, aby włączyć automatyczne wyszukiwanie wskaźników ICO na obciążeniach. W przypadku włączenia tej opcji będą też wyświetlane opcje **Działanie po wykryciu** i **Wygeneruj alert**.
Działanie po wykryciu	Wybierz z listy rozwijanej czynność, która zostanie podjęta w odniesieniu do odpowiednich plików w razie wykrycia zagrożenia na obciążeniu: • **Brak czynności** • **Kwarantanna** • **Usuń** • **Izoluj obciążenia**
Wygeneruj alert	Zaznacz to pole wyboru, aby wygenerować alert w przypadku znalezienia wskaźnika IOC na obciążeniu. Alert zostanie wyświetlony na stronie Alerty.

4. Kliknij **Zastosuj**.

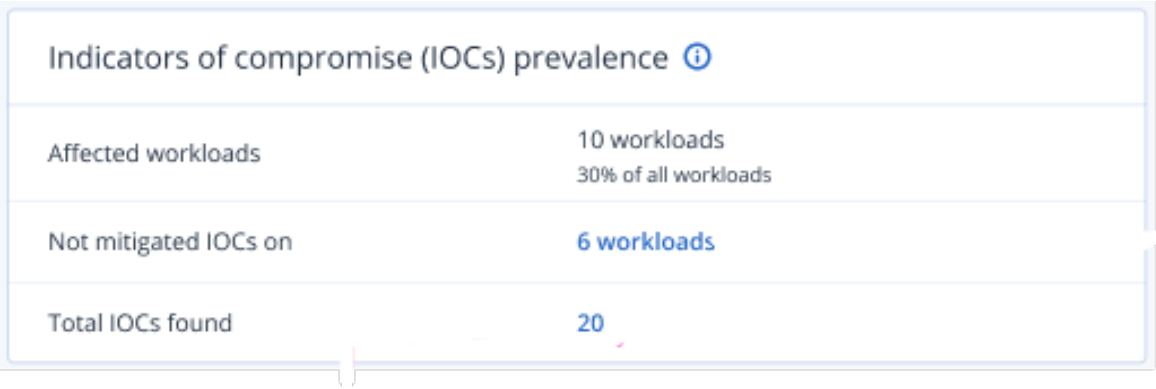
Przeglądanie wskaźników naruszenia zabezpieczeń i niwelowanie skutków na obciążeniach, których dotyczy problem

Jeśli w planie ochrony jest włączony moduł Endpoint Detection and Response (EDR), można wyświetlić wszystkie znane zagrożenia, które wywierają wpływ na obciążenia objęte planem ochrony. Można też zniwelować wszelkie wskaźniki naruszenia zabezpieczeń, które nie zostały zniwelowane automatycznie. Informacje na temat automatycznego niwelowania wskaźników naruszenia zabezpieczeń można znaleźć w sekcji "Określanie ustawień kanałów dotyczących zagrożeń" (s. 999).

Aby przejrzeć obciążenia i zniwelować na nich problemy

1. W konsoli Cyber Protect przejdź do sekcji **Monitorowanie > Kanał dotyczący zagrożeń**.
2. Kliknij zagrożenie, aby wyświetlić szczegółowe informacje na jego temat.
3. W sekcji **Rozpowszechnianie wskaźników naruszenia zabezpieczeń (IOC)** kliknij łącze ***n* obciążeń**, aby wyświetlić obciążenia z niezniwelowanymi wskaźnikami IOC.

© Acronis International GmbH, 2003-2024



4. Na wyświetlonej stronie Obciążenia kliknij odpowiednie obciążenie i przejrzyj jego szczegóły. Możesz uruchomić na obciążeniu określoną funkcję, na przykład zdefiniować dodatkowe adresy URL do odfiltrowania (zobacz sekcję "Filtrowanie adresów URL" (s. 906)) i zablokować złośliwe procesy (zobacz punkt „Wykluczenia” w sekcji "Ustawienia modułu Ochrona przed wirusami i złośliwym oprogramowaniem" (s. 881)).
   Jeśli na przykład kanał dotyczący zagrożeń wskazuje, że w przypadku obciążenia wystąpił wskaźnik IOC, najpierw zlokalizuj i przeanalizuj wskaźnik IOC zgodnie z opisem podanym w sekcji "Przeglądanie i analizowanie wykrytych wskaźników naruszenia zabezpieczeń" (s. 1001). Następnie przejdź do planu ochrony obciążenia i zdefiniuj dodatkową ochronę, na przykład blokowanie złośliwych skrótów plików lub procesów.

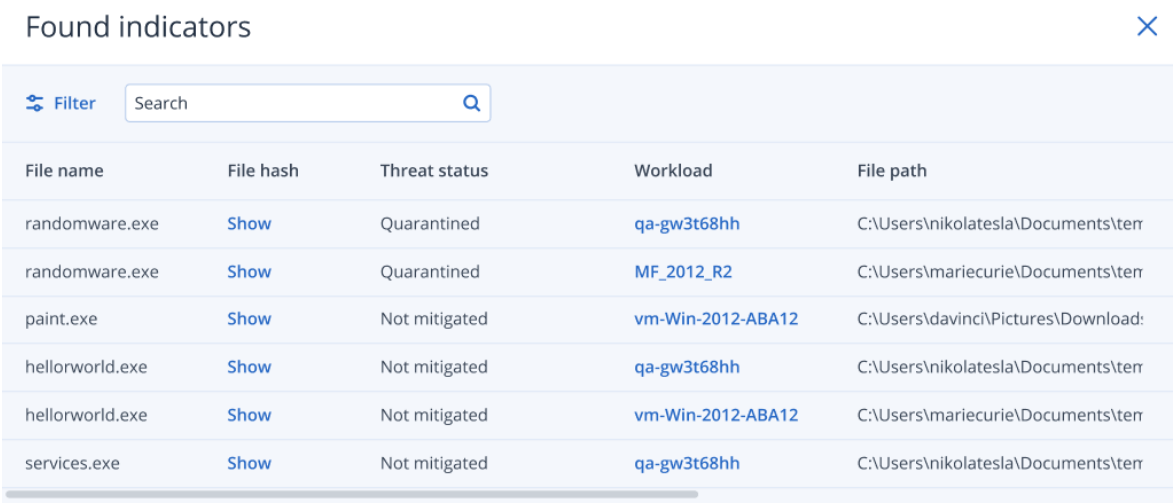
Przeglądanie i analizowanie wykrytych wskaźników naruszenia zabezpieczeń

Oprócz przeglądania obciążeń, które ucierpiały wskutek znanych zagrożeń, można też przeglądać i analizować konkretne wskaźniki naruszenia zabezpieczeń (Indicator of Compromise, IOC). Funkcja ta umożliwia przeglądanie poszczególnych obciążeń, których dotyczy dany wskaźnik IOC, oraz niwelowanie skutków tego wskaźnika.

Aby przejrzeć i przeanalizować wskaźniki naruszenia zabezpieczeń

1. W konsoli Cyber Protect przejdź do sekcji **Monitorowanie > Kanał dotyczący zagrożeń**.
2. Kliknij zagrożenie, aby wyświetlić szczegółowe informacje na jego temat.
3. W sekcji **Rozpowszechnianie wskaźników naruszenia zabezpieczeń (IOC)** kliknij łącze **Łączna liczba znalezionych wskaźników naruszenia zabezpieczeń**.
   Zostanie wyświetlona strona Znalezione wskaźniki.

© Acronis International GmbH, 2003-2024



4. (Opcjonalnie) Skorzystaj z opcji **Filtruj**, aby przefiltrować listę wskaźników IOC według ich statusów. Możesz też skorzystać z opcji **Szukaj**, aby wyszukać określone wskaźniki IOC.
5. Aby wyświetlić obciążenie, którego dotyczy dany wskaźnik IOC, kliknij łącze w kolumnie **Obciążenie**. Następnie możesz wykonać w odniesieniu do obciążenia różne czynności, na przykład uruchomić zarządzanie poprawkami lub zmodyfikować plan ochrony.
6. (Opcjonalnie) W kolumnie **Skrót pliku** kliknij **Pokaż**, aby wyświetlić skróty plików znalezionych w związku z danym wskaźnikiem IOC. W wyświetlonym oknie dialogowym kliknij , aby skopiować skrót pliku związanego z danym wskaźnikiem IOC do edytora tekstów.

Naprawianie incydentów

Moduł Endpoint Detection and Response (EDR) umożliwia wykonywanie czynności naprawczych w odniesieniu do całych incydentów lub poszczególnych punktów ataku w ramach incydentu.

W ramach naprawiania całego incydentu można wybrać czynności naprawcze, które mają zostać wykonane globalnie w odniesieniu do incydentu. Jeśli chcesz precyzyjniej zarządzać incydentem, możesz naprawiać pojedyncze punkty ataku stosownie do potrzeb. Możesz na przykład odizolować sieć obciążenia, aby zatrzymać przenoszenie się ataku w ramach środowiska lub działania C&C (Command & Control) — mimo odizolowania obciążenia wszystkie technologie rozwiązania Acronis Cyber Protect będą nadal działać i będzie można prowadzić dochodzenie.

Moduł EDR zapewnia skuteczne metody naprawiania w ramach następujących operacji:

- Niwelowanie — aby zapewnić zatrzymanie zagrożenia.
- Odzyskiwanie — aby zapewnić niezwłoczną ponowną dostępność usług w trybie online.
- Zapobieganie — aby zapewnić, że technik użytych do ataku nie będzie można ponownie użyć podczas kolejnych ataków.

Naprawianie całego incydentu

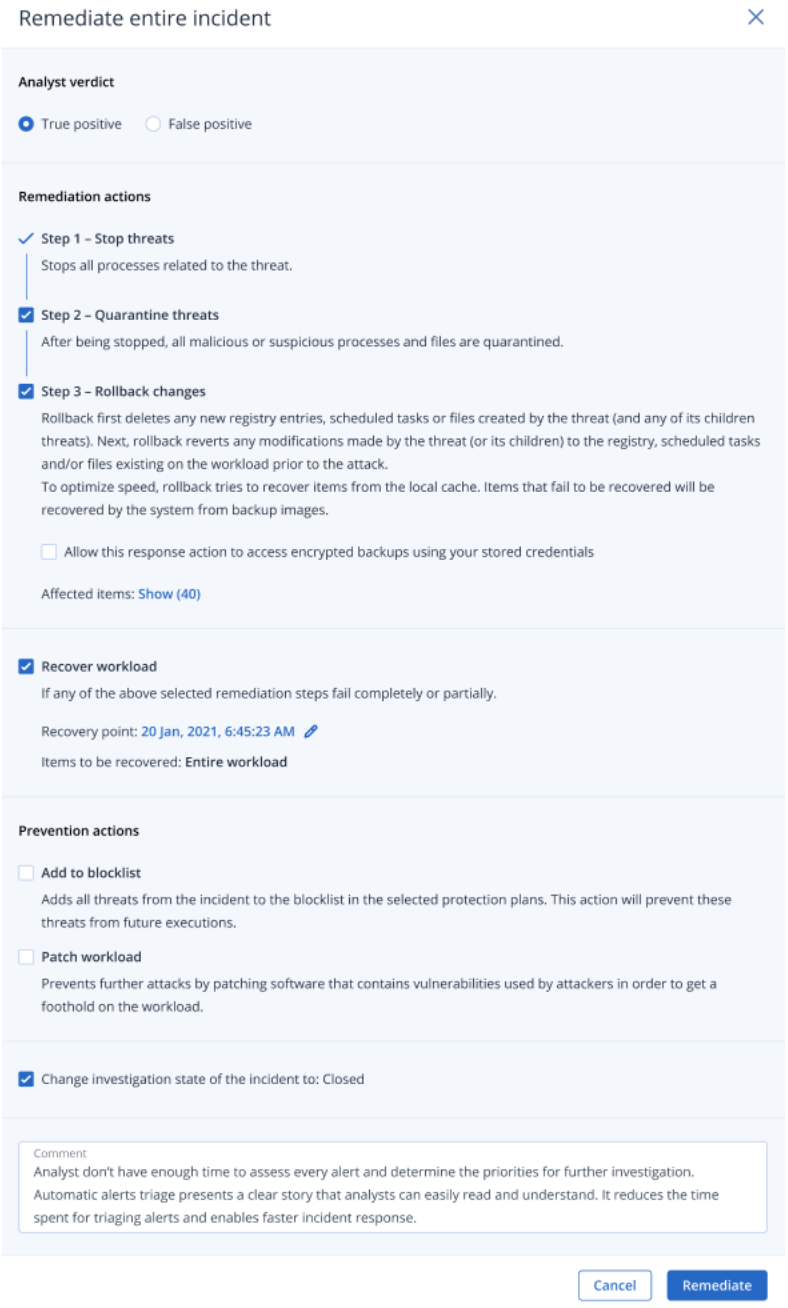
W ramach naprawiania całego incydentu można szybko i łatwo wybrać czynności naprawcze, które mają zostać wykonane globalnie w odniesieniu do incydentu. Moduł Endpoint Detection and Response (EDR) prowadzi krok po kroku przez proces naprawczy.

© Acronis International GmbH, 2003-2024

Jeśli potrzebujesz precyzyjniejszego zarządzania siecią i incydentem, zobacz sekcję "Czynności w ramach reagowania dotyczące indywidualnych węzłów z cybernetycznego łańcucha zabijania" (s. 1007).

Aby naprawić cały incydent

1. W konsoli Cyber Protect przejdź do sekcji **Ochrona > Incydenty**.
2. Na wyświetlonej liście incydentów kliknij w pierwszej kolumnie z prawej strony w obszarze incydentu, który chcesz poddać dochodzeniu. Zostanie wyświetlony cybernetyczny łańcuch zabijania dotyczący wybranego incydentu.
3. Kliknij **Napraw cały incydent**. Zostanie wyświetlone okno dialogowe Napraw cały incydent.



© Acronis International GmbH, 2003-2024

4. W sekcji **Werdykt analityków** na podstawie wyników dochodzenia w sprawie incydentu wybierz jedną z następujących opcji:
   - **Prawdziwe zgłoszenie**: Wybierz tę opcję, jeśli masz pewność, że chodzi o prawdziwy atak. Po wybraniu tej opcji możesz dodać czynności naprawcze i zapobiegawcze zgodnie z opisem podanym w kolejnych krokach.
   - **Fałszywe zgłoszenie**: Wybierz tę opcję, jeśli masz pewność, że nie chodzi o prawdziwy atak. W tym trybie można zapobiec ponownemu zgłoszeniu takiej sytuacji, na przykład przez dodanie incydentu do listy dozwolonych w planie ochrony.

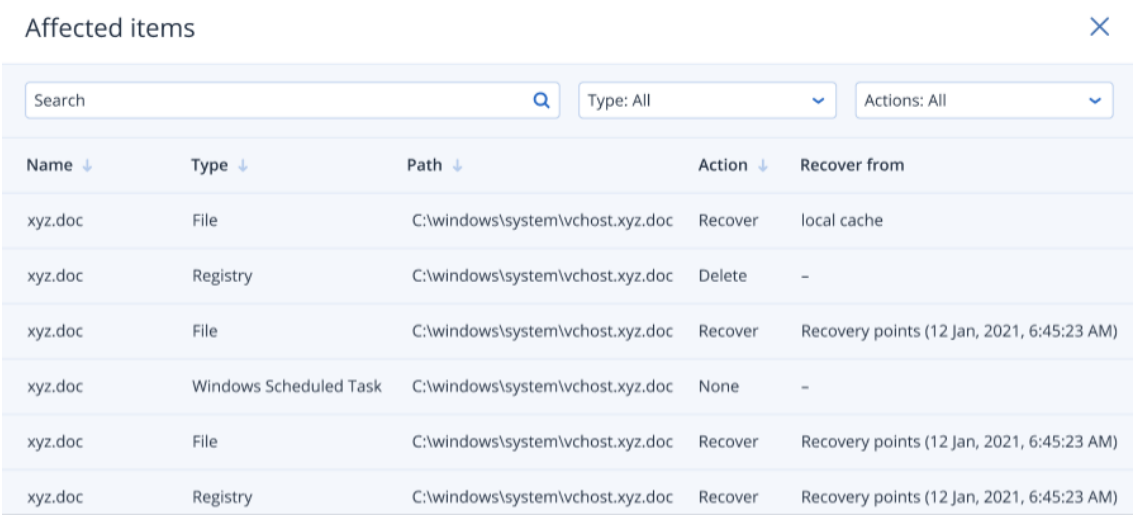
     Uwaga
     W przypadku zaznaczenia opcji **Fałszywe zgłoszenie** można zdefiniować tylko czynności zapobiegawcze. Aby uzyskać więcej informacji, zobacz "Naprawianie incydentów z fałszywych zgłoszeń" (s. 1006).

5. W sekcji **Czynności naprawcze** wykonaj następujące kroki naprawcze. Pamiętaj, że trzeba je wykonać po kolei, czyli nie można na przykład wybrać kroku 2 przed ukończeniem kroku 1.
   a. **Krok 1 — zatrzymaj zagrożenia**: Zaznacz to pole wyboru, aby zatrzymać wszystkie procesy związane z danym zagrożeniem.
   b. **Krok 2 — poddaj zagrożenia kwarantannie**: Po zatrzymaniu zagrożenia zaznacz to pole wyboru, aby poddać kwarantannie wszystkie złośliwe i podejrzane procesy oraz pliki.
   c. **Krok 3 — wycofaj zmiany**: Po poddaniu zagrożenia kwarantannie zaznacz to pole wyboru, aby usunąć wszystkie nowe wpisy rejestru, zaplanowane zadania lub pliki utworzone przez zagrożenie (i wszystkie jego zagrożenia podrzędne). Wówczas proces wycofywania cofnie wszelkie modyfikacje dokonane przez zagrożenie (lub jego zagrożenia podrzędne) w rejestrze, zaplanowanych zadaniach i/lub plikach istniejących na obciążeniu przed atakiem. Aby zoptymalizować szybkość, w ramach procesu wycofywania zostanie podjęta próba odzyskania elementów z lokalnej pamięci podręcznej. Elementy, których nie uda się odzyskać, zostaną odzyskane przez system z obrazów kopii zapasowych.

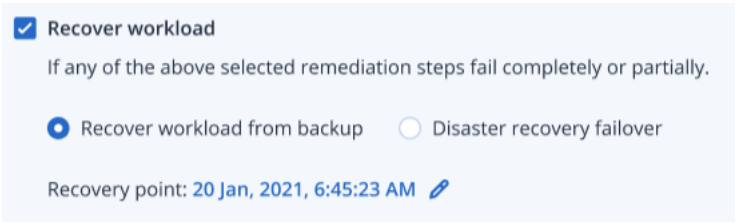
      Uwaga
      Proces wycofywania odzyskuje dane wyłącznie z elementów bufora lokalnego. Wycofywanie z archiwów kopii zapasowych będzie dostępne w przyszłych wersjach.

      Zaznacz pole wyboru **Zezwól tej czynności w ramach reagowania na dostęp do zaszyfrowanych kopii zapasowych przy użyciu przechowywanych poświadczeń**, jeśli dostęp do odpowiednich kopii zapasowych jest szyfrowany. EDR uzyskuje dostęp do przechowywanych poświadczeń użytkownika w celu odszyfrowania archiwów zaszyfrowanych i wyszukania odpowiednich plików.
      Możesz też kliknąć **Elementy, których dotyczy problem**, aby wyświetlić wszystkie elementy (pliki, rejestr lub zaplanowane zadania) objęte operacją wycofywania, zastosowane czynności (**Usuń**, **Odzyskaj** lub **Brak**) oraz informacje, czy dane elementy są przywracane z lokalnej pamięci podręcznej, czy z obrazów kopii zapasowych.

© Acronis International GmbH, 2003-2024



d. **Odzyskaj obciążenie**: Zaznacz to pole wyboru, aby odzyskać obciążenie, jeśli którykolwiek z powyższych kroków naprawczych się nie powiedzie (całkowicie lub częściowo).



Wybierz jedną z następujących opcji odzyskiwania:

- **Odzyskaj obciążenie z kopii zapasowej**: Umożliwia odzyskanie obciążenia z określonego punktu odzyskiwania. Kliknij ikonę edycji punktu odzyskiwania, aby go wybrać z listy kopii zapasowych do odzyskania.
- **Przełączanie awaryjne w ramach odzyskiwania po awarii**: Umożliwia uruchomienie odzyskiwania po awarii, jeśli ta funkcja jest włączona w planie ochrony. Zalecamy korzystanie z tej opcji w przypadku krytycznych obciążeń, takich jak serwery AD czy serwery baz danych. Aby uzyskać więcej informacji, zobacz "Wdrażanie funkcji odzyskiwania po awarii" (s. 786).

6. W sekcji **Czynności mające na celu zapobieganie** wybierz odpowiednie kroki naprawcze:
   - **Dodaj do listy zablokowanych**: Zaznacz to pole wyboru i z wyświetlonej listy planów ochrony wybierz odpowiednie plany ochrony. Ta czynność zapobiegawcza spowoduje zablokowanie wykrywania danego incydentu w ramach wybranych planów ochrony.
   - **Zastosuj poprawkę do obciążenia**: Zaznacz to pole wyboru, aby zainstalować poprawki do każdego oprogramowania, które ma luki w zabezpieczeniach, i uniemożliwić hakerom uzyskanie dostępu do obciążenia. Po zainstalowaniu poprawek możesz wybrać odpowiednią czynność do wykonania (**Nie uruchamiaj ponownie**, **Uruchom ponownie** lub **Uruchom ponownie tylko w razie konieczności**) — w zależności od tego, czy jest zalogowany użytkownik.
     Możesz też zaznaczyć pole wyboru **Nie uruchamiaj ponownie podczas tworzenia kopii zapasowej**, aby się upewnić, że obciążenie nie zostanie uruchomione ponownie w trakcie operacji tworzenia kopii zapasowej.

© Acronis International GmbH, 2003-2024

7. Zaznacz pole wyboru **Zmień stan dochodzenia w sprawie incydentu na: Zamknięto**. Jeśli to pole wyboru nie zostanie zaznaczone, zostanie zachowany poprzedni stan dochodzenia.
8. Kliknij **Napraw**. Wybrane czynności naprawcze są wykonywane po kolei, a postęp realizacji każdej z nich jest wyświetlany w oknie dialogowym Napraw cały incydent.
   Po kliknięciu napis na przycisku zostanie zmieniony na **Przejdź do działań**. Kliknij **Przejdź do działań**, aby przejrzeć wszystkie czynności zastosowane do incydentu w ramach reakcji. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Naprawianie incydentów z fałszywych zgłoszeń

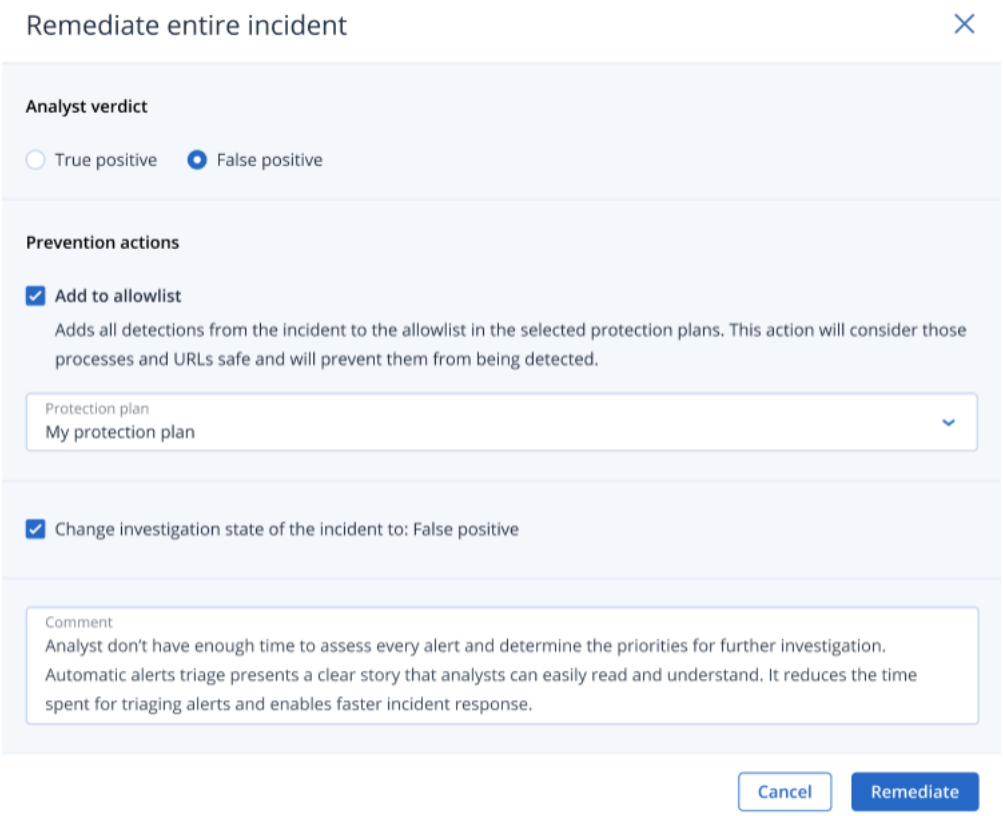
Jeśli masz pewność, że dany incydent nie jest prawdziwym atakiem, czyli został niepotrzebnie zgłoszony, możesz zapobiec powtórnemu zgłoszeniu takiego incydentu. Możesz na przykład dodać incydent do listy dozwolonych w planie ochrony.

Aby naprawić incydent z fałszywego zgłoszenia

1. W cybernetycznym łańcuchu zabijania znajdź dany incydent i kliknij widoczne obok niego pole wyboru **Napraw cały incydent**. Zostanie wyświetlone okno dialogowe Napraw cały incydent.

© Acronis International GmbH, 2003-2024

2. W sekcji **Werdykt analityków** wybierz **Fałszywe zgłoszenie**.



3. W sekcji **Czynności mające na celu zapobieganie** zaznacz pole wyboru **Dodaj do listy dozwolonych**. Z wyświetlonej listy planów ochrony wybierz odpowiednie plany ochrony. Ta czynność zapobiegawcza sprawi, że dany incydent nie będzie wykrywany w ramach wybranych planów ochrony.
4. Zaznacz pole wyboru **Zmień stan dochodzenia w sprawie incydentu na: Fałszywe zgłoszenie**.
5. Kliknij **Napraw**.
   Po kliknięciu napis na przycisku zostanie zmieniony na **Przejdź do działań**. Kliknij **Przejdź do działań**, aby przejrzeć czynności zastosowane do incydentu w ramach reakcji. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Czynności w ramach reagowania dotyczące indywidualnych węzłów z cybernetycznego łańcucha zabijania

Jeśli chcesz precyzyjniej zarządzać incydentem, możesz w ramach reagowania stosować różne czynności do pojedynczych węzłów z cybernetycznego łańcucha zabijania. Te czynności w ramach reagowania umożliwiają szybkie i łatwe naprawienie każdego węzła.

Uwaga
Jeśli w ramach reagowania chcesz zastosować czynności globalnie do całego incydentu, zobacz sekcję "Naprawianie całego incydentu" (s. 1002).

© Acronis International GmbH, 2003-2024

Czynności podejmowane w ramach reagowania dzielą się na następujące kategorie, choć nie wszystkie węzły obejmują wszystkie poniższe kategorie:

- **Napraw**: Czynności z tej kategorii umożliwiają natychmiastową reakcję na atak i obejmują zarządzanie izolacją obciążenia od sieci, a także usuwanie plików, procesów oraz wartości rejestru i poddawanie ich kwarantannie.
- **Przeprowadź dochodzenie**: Czynności z tej kategorii (dotyczące tylko obciążeń) umożliwiają uruchomienie operacji tworzenia kopii zapasowej na potrzeby analizy śledczej lub połączenie pulpitu zdalnego w celu przeprowadzenia dokładniejszego dochodzenia.
- **Przeprowadź dochodzenie**: Czynności z tej kategorii (dotyczące tylko obciążeń) umożliwiają nawiązanie połączenia z pulpitem zdalnym w celu przeprowadzenia dokładniejszego dochodzenia.
- **Odzyskiwanie**: Czynności z tej kategorii (dotyczące tylko obciążeń) umożliwiają reagowanie na intensywne ataki przez uruchomienie odzyskiwania z kopii zapasowej lub przełączenia awaryjnego w ramach odzyskiwania po awarii.
- **Zapobiegaj**: Czynności z tej kategorii umożliwiają zapobieganie przyszłym zagrożeniom lub fałszywym zgłoszeniom incydentów przez dodanie ich do listy dozwolonych lub listy zablokowanych w planie ochrony.

Uwaga
Jeśli incydent zostanie zamknięty, nie można wykonać czynności w ramach reagowania względem węzła. Jednakże możliwe jest ponowne otwarcie zamkniętego zdarzenia poprzez zmianę jego stanu dochodzenia na **Trwa dochodzenie**. Po ponownym otwarciu możliwe jest wykonanie czynności w ramach reagowania.

W poniższej tabeli opisano każdy typ węzłów w cybernetycznym łańcuchu zabijania, kategorie mające zastosowanie do poszczególnych węzłów, a także dostępne czynności w ramach reagowania.

Węzeł	Kategoria	Czynności w ramach reagowania
Obciążenie	Napraw	• Zarządzaj izolacją sieci • Uruchom ponownie obciążenie
	Przeprowadź dochodzenie	• Kopia zapasowa na potrzeby analizy śledczej • Połączenie pulpitu zdalnego
	Przeprowadź dochodzenie	• Połączenie pulpitu zdalnego

© Acronis International GmbH, 2003-2024

Węzeł	Kategoria	Czynności w ramach reagowania
	Odzyskiwanie	• Odzyskiwanie z kopii zapasowej • Przełączanie awaryjne w ramach odzyskiwania po awarii
	Zapobiegaj	• Zastosuj poprawkę
Proces	Napraw	• Zatrzymaj proces • Kwarantanna
	Zapobiegaj	• Dodaj do listy dozwolonych • Dodaj do listy zablokowanych
Plik	Napraw	• Usuń • Kwarantanna
	Zapobiegaj	• Dodaj do listy dozwolonych • Dodaj do listy zablokowanych
Rejestr	Napraw	• Usuń
Sieć	Zapobiegaj	• Dodaj do listy dozwolonych • Dodaj do listy zablokowanych

Definiowanie czynności w ramach reagowania dotyczących obciążeń, które ucierpiały wskutek ataku

W ramach reakcji na atak możesz wykonać następujące czynności w odniesieniu do obciążeń, które ucierpiały wskutek ataku:

- **Zarządzaj izolacją sieci**: Umożliwia zarządzanie izolacją sieci obciążenia w celu zatrzymania przenoszenia ataku w ramach środowiska lub działań Command & Control (C&C). Aby uzyskać więcej informacji, zobacz "Zarządzanie izolacją sieci obciążenia" (s. 1010).

© Acronis International GmbH, 2003-2024

- **Zastosuj poprawkę**: Umożliwia zastosowanie poprawek do obciążenia w celu zapobieżenia wykorzystaniu luk w zabezpieczeniach podczas ewentualnych przyszłych ataków. Aby uzyskać więcej informacji, zobacz "Stosowanie poprawki do obciążenia" (s. 1014).
- **Uruchom ponownie obciążenie**: Umożliwia ponowne uruchomienie obciążenia — niezwłocznie lub według predefiniowanego limitu czasu. Aby uzyskać więcej informacji, zobacz "Ponowne uruchamianie obciążenia" (s. 1016).
- **Kopia zapasowa na potrzeby analizy śledczej**: Umożliwia tworzenie na żądanie kopii zapasowej w celach związanych z audytem lub dalszymi czynnościami śledczymi. Aby uzyskać więcej informacji, zobacz "Tworzenie na żądanie kopii zapasowej na potrzeby analizy śledczej dla obciążenia" (s. 1017).
- **Połączenie pulpitu zdalnego**: Umożliwia zdalny dostęp do badanego obciążenia. Aby uzyskać więcej informacji, zobacz "Połączenie zdalne z obciążeniem" (s. 1018).
- **Odzyskaj z kopii zapasowej**: Umożliwia odzyskanie z kopii zapasowej całego komputera lub określonych plików bądź folderów. Aby uzyskać więcej informacji, zobacz "Odzyskiwanie z kopii zapasowej" (s. 1019).
- **Przełączanie awaryjne w ramach odzyskiwania po awarii**: Umożliwia uruchomienie operacji "Wdrażanie funkcji odzyskiwania po awarii" (s. 786). Należy pamiętać, że obciążenie musi mieć subskrypcję usługi Zaawansowane odzyskiwanie po awarii. Aby uzyskać więcej informacji, zobacz "Przełączanie awaryjne w ramach odzyskiwania po awarii" (s. 1020).

Zarządzanie izolacją sieci obciążenia

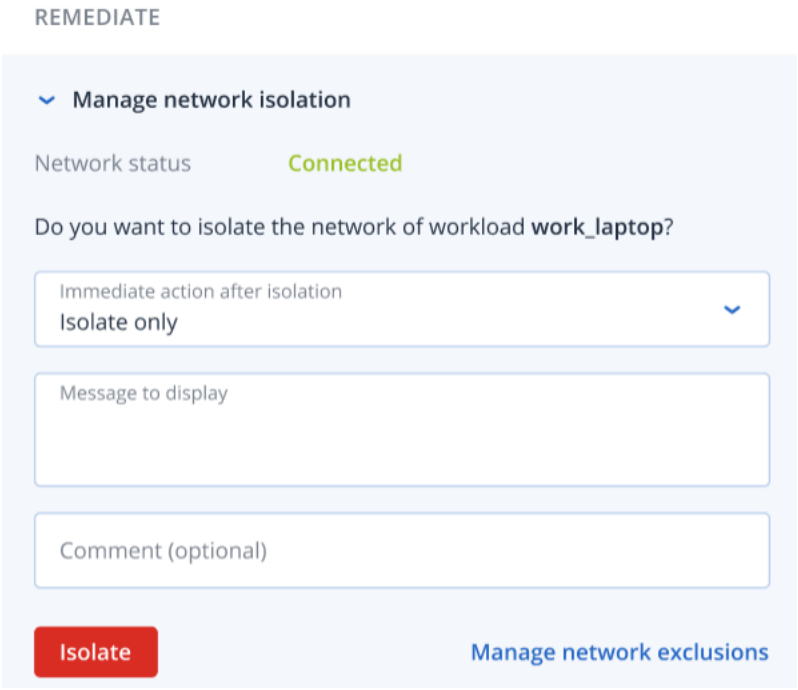
Moduł EDR umożliwia zarządzanie izolacją sieci obciążenia w celu zatrzymania przenoszenia ataku w ramach środowiska lub działań Command & Control (C&C). Dostępne są różne opcje izolacji, które można dobierać stosownie do swoich wymagań. Uwaga: wszystkie technologie rozwiązania Acronis Cyber Protect działają nawet wtedy, gdy obciążenie jest odizolowane, co pozwala na prowadzenie dochodzenia.

Aby odizolować obciążenie od sieci

1. W cybernetycznym łańcuchu zabijania kliknij węzeł obciążenia, który chcesz naprawić.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.

© Acronis International GmbH, 2003-2024

3. W sekcji **Napraw** kliknij **Zarządzaj izolacją sieci**.



Uwaga
Wartość **Status sieci** wskazuje, czy obciążenie jest obecnie połączone. Jeśli jest wyświetlana wartość **Izolowano**, można ponownie połączyć odizolowane obciążenie z siecią, postępując zgodnie z niżej opisaną procedurą. Jeśli obciążenie jest w trybie offline, wciąż można je odizolować. Kiedy obciążenie wróci do trybu online, zostanie automatycznie wprowadzone w stan **Izolowano**.

4. Z listy rozwijanej **Niezwłoczna czynność po izolacji** wybierz jedną z następujących pozycji:
   - **Tylko izoluj**
   - **Izoluj obciążenie i utwórz jego kopię zapasową**
   - **Izoluj obciążenie i utwórz jego kopię zapasową z danymi do analizy śledczej**
   - **Izoluj i wyłącz obciążenie**

   Dodatkowe informacje na temat definiowania miejsca tworzenia kopii zapasowej obciążenia i opcji szyfrowania można znaleźć w sekcji "Zarządzanie tworzeniem kopii zapasowych oraz odzyskiwaniem obciążeń i plików" (s. 424).
5. [Opcjonalnie] W polu **Wiadomość do wyświetlenia** dodaj wiadomość, która będzie wyświetlana dla użytkowników uzyskujących dostęp do odizolowanego obciążenia. Za jej pomocą możesz na przykład poinformować użytkowników, że obciążenie jest odizolowane, w związku z czym dostęp sieciowy do i z tego obciążenia jest obecnie niemożliwy. Pamiętaj, że wiadomość ta jest też wyświetlana jako powiadomienie na pasku zadań, które będzie widoczne, dopóki użytkownik go nie zamknie.
6. [Opcjonalnie] W polu **Komentarz** dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim

© Acronis International GmbH, 2003-2024

współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.

7. Kliknij **Zarządzaj wykluczeniami na poziomie sieci**, aby dodać porty, adresy URL, nazwy hostów i adresy IP, które będą miały dostęp do obciążenia w czasie izolacji. Dodatkowe informacje można znaleźć w sekcji Jak zarządzać wykluczeniami na poziomie sieci.
8. Kliknij **Izoluj**.
   Obciążenie zostanie odizolowane. Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Uwaga
Obciążenie będzie też oznaczone jako **Izolowano** w menu **Obciążenia** w konsoli Cyber Protect. Wybrane obciążenia można też odizolować z poziomu menu **Obciążenia > Obciążenia z agentami**. W tym celu zaznacz odpowiednie obciążenia i na prawym pasku bocznym kliknij **Zarządzaj izolacją sieci**. W wyświetlonym oknie dialogowym można zarządzać wykluczeniami na poziomie sieci i kliknąć **Izoluj** lub **Izoluj wszystkie**, aby odizolować wybrane obciążenia.

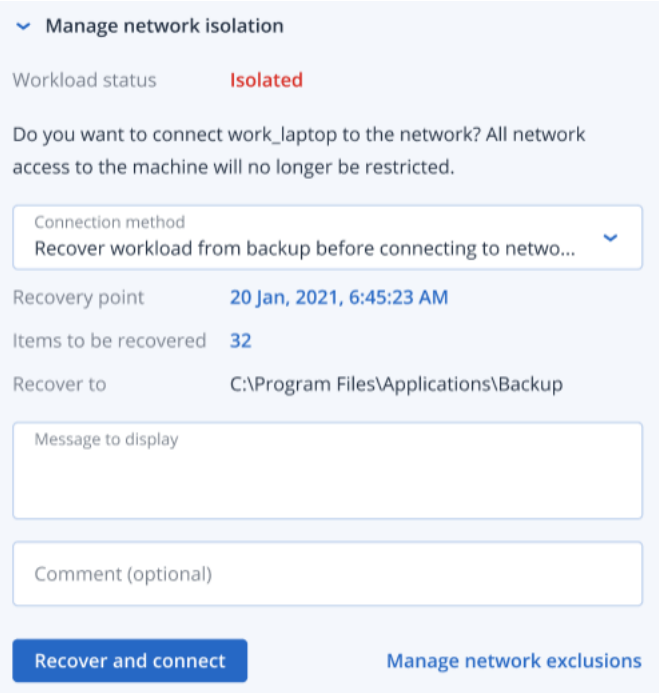
Aby ponownie połączyć odizolowane obciążenie z siecią

1. W cybernetycznym łańcuchu zabijania kliknij węzeł obciążenia, które chcesz ponownie połączyć.

Uwaga
Połączenie z siecią można wznowić nawet wtedy, gdy obciążenie jest w trybie offline — kiedy wróci do trybu online, zostanie automatycznie wprowadzone w stan **Połączono**.

2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Napraw** kliknij **Zarządzaj izolacją sieci**.
4. Wybierz jedną z następujących opcji:
   - **Niezwłocznie nawiąż połączenie z siecią**: obciążenie zostanie ponownie połączone z siecią.
   - **Odzyskaj obciążenie z kopii zapasowej, zanim nawiążesz połączenie z siecią**: wybierz punkt odzyskiwania, z którego chcesz odzyskać obciążenie.
     a. W polu **Punkt odzyskiwania** kliknij **Wybierz**.
     b. Na wyświetlonym pasku bocznym wybierz odpowiedni punkt odzyskiwania.
     c. Kliknij **Odzyskaj > Całe obciążenie**, aby odzyskać wszystkie pliki i foldery obciążenia.
     lub
     Kliknij **Odzyskaj > Pliki i foldery**, aby odzyskać wybrane pliki i foldery obciążenia. Następnie zostanie wyświetlony monit o wybranie odpowiednich plików lub folderów. Po ich wybraniu można wyświetlić listę elementów, klikając odpowiednią wartość w polu **Elementy do odzyskania**.

© Acronis International GmbH, 2003-2024



Uwaga
Jeśli wybrany punkt odzyskiwania jest zaszyfrowany, zostanie wyświetlony monit o podanie hasła.

5. [Opcjonalnie] Zaznacz pole wyboru **W razie potrzeby uruchom ponownie obciążenie**. Ta opcja ma zastosowanie tylko w sytuacji, gdy w kroku 4 została wybrana opcja **Odzyskaj > Całe obciążenie**.
6. [Opcjonalnie] W polu **Wiadomość do wyświetlenia** dodaj wiadomość, która będzie wyświetlana dla użytkowników uzyskujących dostęp do połączonego obciążenia. Możesz na przykład poinformować użytkowników, że na obciążenie przywrócono kopię zapasową oraz wznowiono dostęp sieciowy do i z obciążenia.
7. [Opcjonalnie] W polu **Komentarz** dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
8. Kliknij **Połącz**, jeśli w kroku 4 została wybrana opcja **Niezwłocznie nawiąż połączenie z siecią**.
   lub
   Kliknij **Odzyskaj i połącz**, jeśli w kroku 4 została wybrana opcja **Odzyskaj obciążenie z kopii zapasowej, zanim nawiążesz połączenie z siecią**.
   Obciążenie zostanie ponownie połączone z siecią, a wszelkie ograniczenia dostępu do i z obciążenia zostaną zniesione.

© Acronis International GmbH, 2003-2024

Uwaga
Wybrane odizolowane obciążenia można też połączyć z poziomu menu **Obciążenia > Obciążenia z agentami** w konsoli Cyber Protect. W tym celu zaznacz odpowiednie obciążenia i na prawym pasku bocznym kliknij **Zarządzaj izolacją sieci**. W wyświetlonym oknie dialogowym kliknij **Połącz** lub **Połącz wszystkie**, aby wznowić połączenie wybranych obciążeń z siecią.

Aby zarządzać wykluczeniami na poziomie sieci

Uwaga
Mimo że wszystkie technologie rozwiązania Acronis Cyber Protect działają w czasie izolacji obciążenia, może wystąpić konieczność nawiązania dodatkowego połączenia z siecią (na przykład w celu przesłania pliku z obciążenia do współdzielonego katalogu). W takiej sytuacji można dodać wykluczenie na poziomie sieci, ale najpierw należy dopilnować, aby zostały usunięte wszystkie zagrożenia.

1. W sekcji **Napraw** na karcie **Czynności w ramach reagowania** kliknij **Zarządzaj wykluczeniami na poziomie sieci**.
2. Na pasku bocznym Wykluczenia na poziomie sieci dodaj odpowiednie wykluczenia. W przypadku każdej z dostępnych opcji (Porty, Adres URL oraz Nazwa hosta / adres IP) wykonaj następujące czynności:
   a. Kliknij **Dodaj**, a następnie wprowadź odpowiednie porty, adresy URL albo nazwy hostów bądź adresy IP.
   b. Na liście rozwijanej **Kierunek ruchu** wybierz **Połączenia przychodzące i wychodzące**, **Tylko połączenia przychodzące** lub **Tylko połączenia wychodzące**.
   c. Kliknij **Dodaj**.
3. Kliknij **Zapisz**.

Stosowanie poprawki do obciążenia

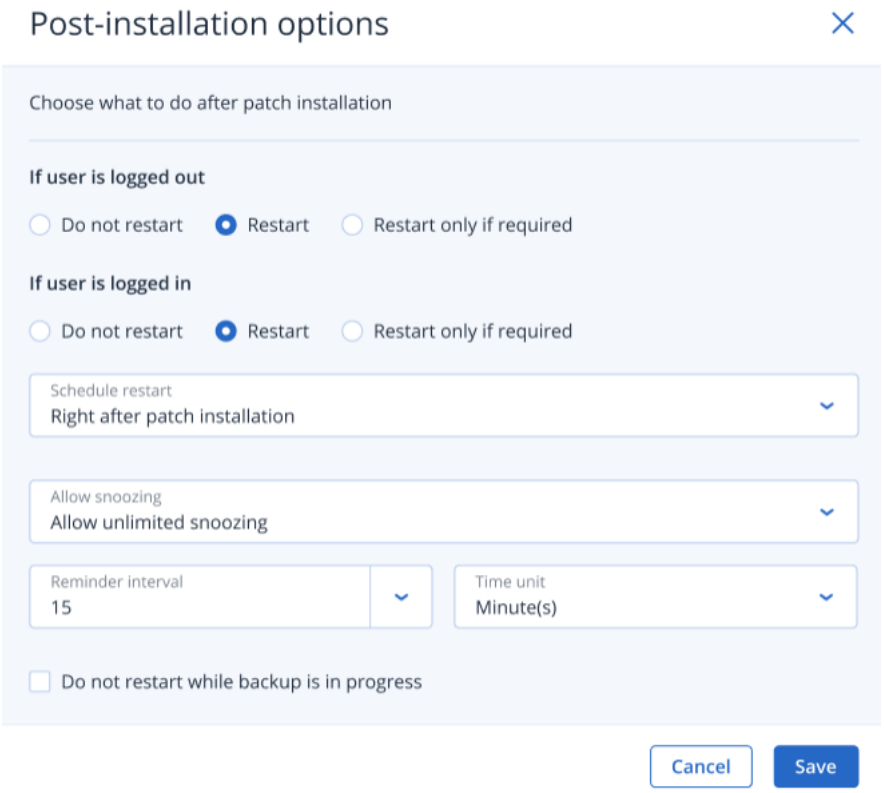
Moduł EDR automatycznie wykrywa, czy dane obciążenie wymaga poprawki, i umożliwia jej zastosowanie w celu zapobieżenia wykorzystaniu luk w zabezpieczeniach podczas ewentualnych przyszłych ataków. Należy pamiętać, że ta funkcja jest dostępna tylko wtedy, gdy obciążenie partnera ma subskrypcję usługi Zarządzanie zaawansowane.

Aby zastosować poprawkę do obciążenia

1. W cybernetycznym łańcuchu zabijania kliknij węzeł obciążenia, na którym chcesz zainstalować poprawkę.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Napraw** kliknij **Zastosuj poprawkę**.
4. W polu **Poprawki do zainstalowania** kliknij **Wybierz**. W wyświetlonym oknie dialogowym zaznacz odpowiednie poprawki, a następnie kliknij **Wybierz**.

© Acronis International GmbH, 2003-2024

5. W polu **Opcje poinstalacyjne** kliknij widoczne tam łącze. Zostanie wyświetlone okno dialogowe Opcje poinstalacyjne.



6. Wybierz czynność, która ma zostać wykonana po zainstalowaniu poprawki:
   - **Jeśli użytkownik się wylogował**: wybierz **Nie uruchamiaj ponownie**, **Uruchom ponownie** lub **Uruchom ponownie tylko w razie konieczności**.
   - **Jeśli użytkownik się zalogował**: wybierz **Nie uruchamiaj ponownie**, **Uruchom ponownie** lub **Uruchom ponownie tylko w razie konieczności**.
     W przypadku wybrania opcji **Uruchom ponownie** możesz też:
     - Zaplanować ponowne uruchomienie.
     - Zezwolić na stosowanie funkcji drzemki, w tym określić odstępy czasowe między drzemkami.
7. [Opcjonalnie] Zaznacz pole wyboru **Nie uruchamiaj ponownie podczas tworzenia kopii zapasowej**, aby się upewnić, że obciążenie nie zostanie uruchomione ponownie w trakcie operacji tworzenia kopii zapasowej.
8. Kliknij **Zapisz**.
9. Na karcie **Czynności w ramach reagowania** kliknij **Zastosuj poprawkę**.
   Zostanie uruchomiona instalacja wybranej poprawki. Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

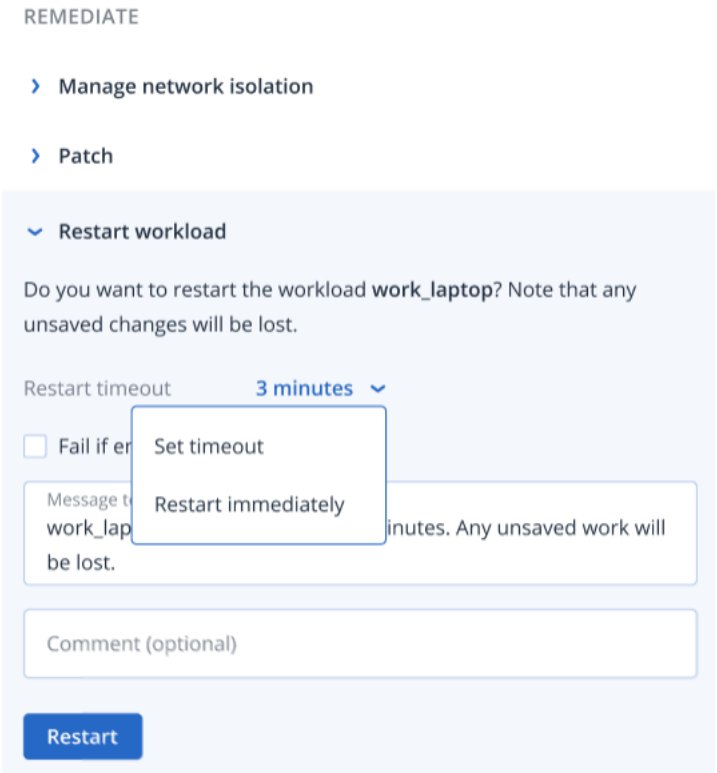
© Acronis International GmbH, 2003-2024

Ponowne uruchamianie obciążenia

W ramach działań naprawczych podejmowanych w reakcji na atak moduł EDR umożliwia ponowne uruchomienie obciążenia — niezwłocznie lub według predefiniowanego limitu czasu.

Aby uruchomić ponownie obciążenie

1. W cybernetycznym łańcuchu zabijania kliknij węzeł obciążenia, dla którego chcesz określić harmonogram ponownego uruchamiania.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Napraw** kliknij **Uruchom ponownie obciążenie**.



4. W polu **Limit czasu ponownego uruchomienia** kliknij wyświetlone łącze, a następnie wybierz jedną z następujących opcji:
   - **Ustaw limit czasu**: W oknie dialogowym Limit czasu ponownego uruchomienia ustaw odstęp czasowy ponownego uruchamiania dla danego obciążenia, a następnie kliknij **Zapisz**.
   - **Niezwłocznie uruchom ponownie**: zaznacz tę opcję, aby niezwłocznie uruchomić ponownie obciążenie.
5. [Opcjonalnie] Zaznacz pole wyboru **Zakończ niepowodzeniem, jeśli jest zalogowany użytkownik**, aby zapobiec ponownemu uruchomieniu obciążenia w sytuacji, gdy jest zalogowany użytkownik.
6. W polu **Wiadomość do wyświetlenia** dodaj wiadomość, która będzie wyświetlana dla użytkowników uzyskujących dostęp do odizolowanego obciążenia.
7. [Opcjonalnie] W polu **Komentarz** dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim

© Acronis International GmbH, 2003-2024

współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.

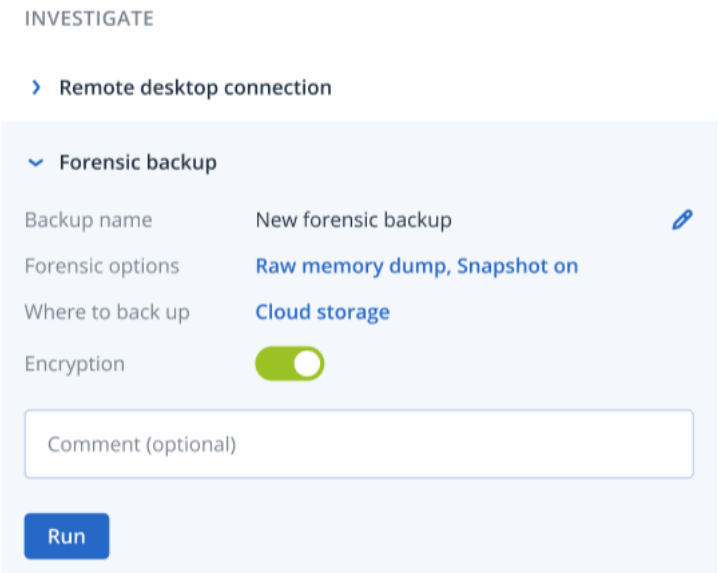
8. Kliknij **Uruchom ponownie**.
   Obciążenie ma skonfigurowane operacje ponownego uruchamiania zgodnie ze zdefiniowanym harmonogramem. Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Tworzenie na żądanie kopii zapasowej na potrzeby analizy śledczej dla obciążenia

W ramach analizy śledczej związanej z atakiem moduł EDR umożliwia uruchomienie na żądanie operacji tworzenia kopii zapasowej w celach związanych z audytem lub dalszymi czynnościami śledczymi. Należy pamiętać, że ta funkcja jest dostępna tylko wtedy, gdy obciążenie partnera ma subskrypcję usługi Zaawansowane tworzenie kopii zapasowych.

Aby uruchomić tworzenie kopii zapasowej na potrzeby analizy śledczej

1. W cybernetycznym łańcuchu zabijania kliknij węzeł obciążenia, na którym chcesz uruchomić tworzenie kopii zapasowej na potrzeby analizy śledczej.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Przeprowadź dochodzenie** kliknij opcję **Kopia zapasowa na potrzeby analizy śledczej**.



4. [Opcjonalnie] W polu **Nazwa kopii zapasowej** kliknij ikonę edycji, aby zmienić nazwę kopii zapasowej.
5. W polu **Opcje analizy śledczej** kliknij widoczne tam łącze. Wyświetlone zostanie okno dialogowe Opcje analizy śledczej, w którym należy wybrać jedną z opcji:
   - **Zapisz surowy zrzut pamięci**
   - **Zapisz zrzut pamięci jądra**

© Acronis International GmbH, 2003-2024

Możesz również zaznaczyć pole wyboru **Migawka uruchomionych procesów**, aby dodać informacje o procesach działających w momencie rozpoczęcia tworzenia kopii zapasowej. Te informacje są zapisywane w obrazie kopii zapasowej.

Kliknij opcję **Zapisz**, aby zamknąć okno dialogowe opcji analizy śledczej.

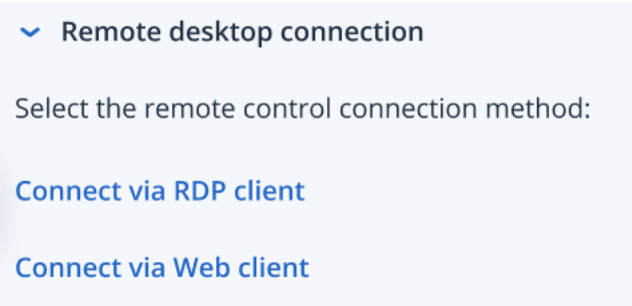
6. W polu **Lokalizacja docelowa kopii zapasowej** kliknij łącze w celu określenia miejsca zapisania kopii zapasowej.
7. [Opcjonalnie] Kliknij opcję **Szyfrowanie**, aby włączyć opcję szyfrowania. W wyświetlonym oknie dialogowym wprowadź hasło do szyfrowanej kopii zapasowej i wybierz odpowiedni algorytm szyfrowania.
8. [Opcjonalnie] W polu **Komentarz** dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
9. Kliknij opcję **Uruchom**.
   Rozpocznie się proces tworzenia kopii zapasowej na potrzeby analizy śledczej. Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Połączenie zdalne z obciążeniem

W ramach analizy śledczej związanej z atakiem moduł EDR umożliwia zdalny dostęp do badanego obciążenia.

Aby nawiązać połączenie zdalne z obciążeniem

1. W cybernetycznym łańcuchu zabijania kliknij węzeł obciążenia, z którym chcesz nawiązać połączenie.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Przeprowadź dochodzenie** kliknij opcję **Podłączanie pulpitu zdalnego**.



4. Wybierz jedną z następujących metod połączenia zdalnego:
   - **Połącz przez klienta RDP**: W tej metodzie pojawi się monit o pobranie i zainstalowanie klienta usługi Podłączanie pulpitu zdalnego. Następnie można nawiązać zdalne połączenie z obciążeniem z konsoli Cyber Protect.

© Acronis International GmbH, 2003-2024

- **Połącz przez klienta internetowego**: W tej metodzie nie ma potrzeby instalowania klienta RDP dla obciążenia. Nastąpi przekierowanie do ekranu logowania, gdzie należy wprowadzić poświadczenia dostępu do komputera zdalnego.

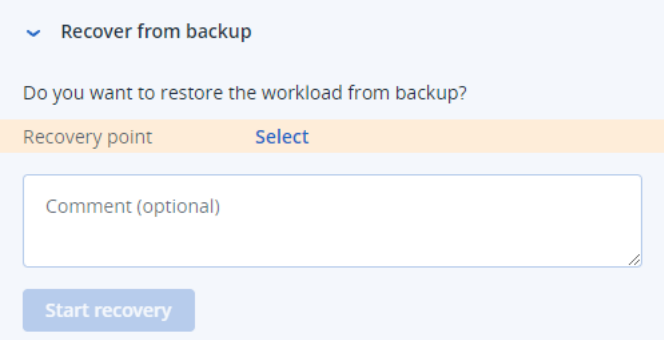
Po nawiązaniu połączenia zdalnego można zobaczyć informacje o tej operacji na karcie **Działania** zarówno dla pojedynczego węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Odzyskiwanie z kopii zapasowej

W ramach reakcji na atak z zastosowaniem odzyskiwania moduł EDR umożliwia odzyskanie z kopii zapasowej albo całego komputera, albo określonych plików lub folderów.

Aby odzyskać obciążenie z kopii zapasowej

1. W cybernetycznym łańcuchu zabijania kliknij węzeł obciążenia, które chcesz odzyskać.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Odzyskiwanie** kliknij **Odzyskaj z kopii zapasowej**.



4. W polu **Punkt odzyskiwania** kliknij **Wybierz**, a następnie:
   a. Na wyświetlonym pasku bocznym wybierz odpowiedni punkt odzyskiwania.
   b. Kliknij **Odzyskaj > Całe obciążenie**, aby odzyskać wszystkie pliki i foldery obciążenia.
   lub
   Kliknij **Odzyskaj > Pliki i foldery**, aby odzyskać wybrane pliki i foldery obciążenia. Następnie zostanie wyświetlony monit o wybranie odpowiednich plików lub folderów. Po ich wybraniu można wyświetlić elementy wybrane do odzyskania, klikając odpowiednią wartość w polu **Elementy do odzyskania**.

   Uwaga
   Jeśli wybrany punkt odzyskiwania jest zaszyfrowany, zostanie wyświetlony monit o podanie hasła.

5. [Opcjonalnie] Zaznacz pole wyboru **Automatycznie uruchom ponownie obciążenie**. Ta opcja ma zastosowanie tylko w sytuacji, gdy w kroku 4 została wybrana opcja **Odzyskaj > Całe obciążenie**.
6. [Opcjonalnie] W polu **Komentarz** dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim

© Acronis International GmbH, 2003-2024

współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.

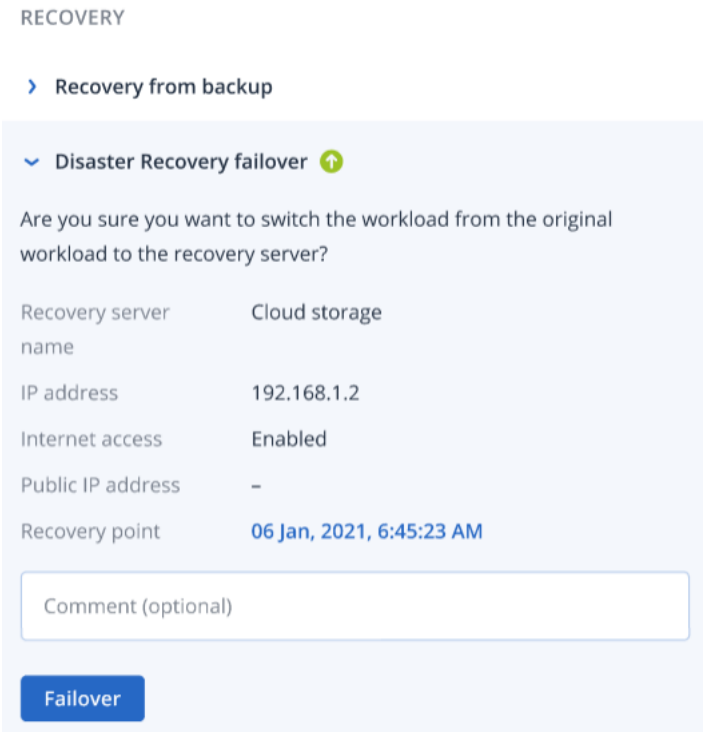
7. Kliknij **Rozpocznij odzyskiwanie**.
   Rozpocznie się proces odzyskiwania obciążenia. Postęp tej czynności będzie widoczny na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Przełączanie awaryjne w ramach odzyskiwania po awarii

W ramach działań naprawczych podejmowanych w reakcji na atak moduł EDR umożliwia uruchomienie operacji "Wdrażanie funkcji odzyskiwania po awarii" (s. 786), co pozwala na przeniesienie obciążenia na serwer odzyskiwania. Należy pamiętać, że obciążenie musi mieć subskrypcję usługi Zaawansowane odzyskiwanie po awarii.

Aby uruchomić przełączanie awaryjne w ramach odzyskiwania po awarii

1. W cybernetycznym łańcuchu zabijania kliknij węzeł obciążenia, które chcesz odzyskać.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Odzyskiwanie** kliknij **Przełączanie awaryjne w ramach odzyskiwania po awarii**.



4. W polu **Punkt odzyskiwania** wykonaj następujące kroki:
   a. Kliknij datę bieżącego punktu odzyskiwania, aby wybrać punkt odzyskiwania.
   b. Na wyświetlonym pasku bocznym wybierz odpowiedni punkt odzyskiwania.

© Acronis International GmbH, 2003-2024

Uwaga
Jeśli masz subskrypcję usługi Zaawansowane odzyskiwanie po awarii, możesz wybrać odpowiedni serwer odzyskiwania (maszynę wirtualną offline) utworzony w usłudze Odzyskiwanie po awarii. Jeśli nie masz subskrypcji, zostanie wyświetlony monit o skonfigurowanie usługi Odzyskiwanie po awarii.

5. [Opcjonalnie] W polu **Komentarz** dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
6. Kliknij **Przełączanie awaryjne**.
   Obciążenie zostanie przeniesione na serwer odzyskiwania. Czynność ta będzie widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Definiowanie czynności w ramach reagowania dotyczących podejrzanego procesu

W ramach działań naprawczych podejmowanych w reakcji na atak możesz wykonać następujące czynności w odniesieniu do podejrzanych procesów:

- Zatrzymanie procesu (zobacz niżej)
- Poddanie procesu kwarantannie (zobacz niżej)
- Wycofanie zmian dokonanych przez proces (zobacz niżej)
- Dodanie procesu do listy dozwolonych lub zablokowanych w planie ochrony (zobacz "Dodawanie lub usuwanie procesu, pliku bądź sieci na liście zablokowanych lub dozwolonych planu ochrony" (s. 1027))

Aby zatrzymać podejrzany proces

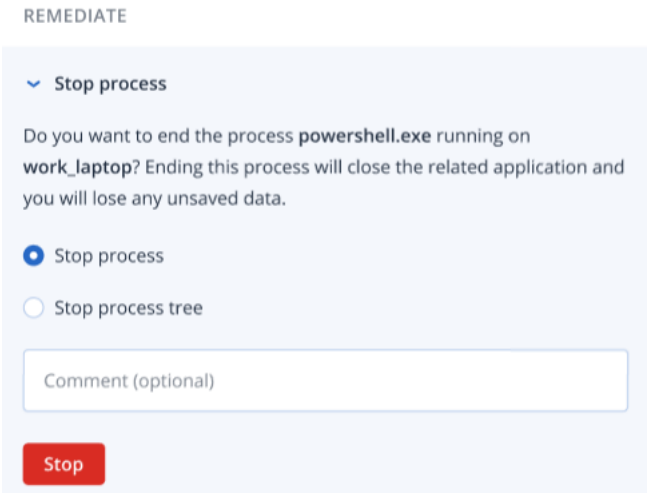
1. W cybernetycznym łańcuchu zabijania kliknij węzeł procesu, który chcesz naprawić.

Uwaga
Krytyczne procesy systemu Windows lub procesy niedziałające nie mogą zostać zatrzymane i są wyłączone w cybernetycznym łańcuchu zabijania.

2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.

© Acronis International GmbH, 2003-2024

3. W sekcji **Napraw** kliknij **Zatrzymaj proces**.



4. Wybierz jedną z następujących opcji:
   - **Zatrzymaj proces** (umożliwia zatrzymanie konkretnego procesu)
   - **Zatrzymaj drzewo procesów** (umożliwia zatrzymanie danego procesu i wszystkich jego procesów podrzędnych)
5. [Opcjonalnie] Dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
6. Kliknij **Zatrzymaj**. Proces zostanie zatrzymany.

Uwaga
Powiązana z nim aplikacja zostanie zamknięta, a wszelkie niezapisane dane zostaną utracone.

Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Aby poddać podejrzany proces kwarantannie

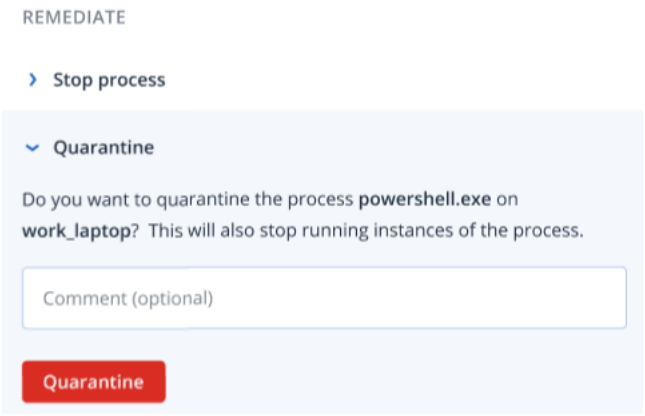
1. W cybernetycznym łańcuchu zabijania kliknij węzeł procesu, który chcesz poddać kwarantannie.

Uwaga
Krytyczne procesy systemu Windows nie mogą zostać poddane kwarantannie i są wyłączone w cybernetycznym łańcuchu zabijania.

2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.

© Acronis International GmbH, 2003-2024

3. W sekcji **Napraw** kliknij **Kwarantanna**.



4. [Opcjonalnie] Dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
5. Kliknij **Kwarantanna**. Proces zostanie zatrzymany, a następnie poddany kwarantannie.

Uwaga
Proces zostanie dodany do sekcji kwarantanny dostępnej w obszarze ochrony przed złośliwym oprogramowaniem i tam też będzie zarządzany.

Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Aby wycofać zmiany

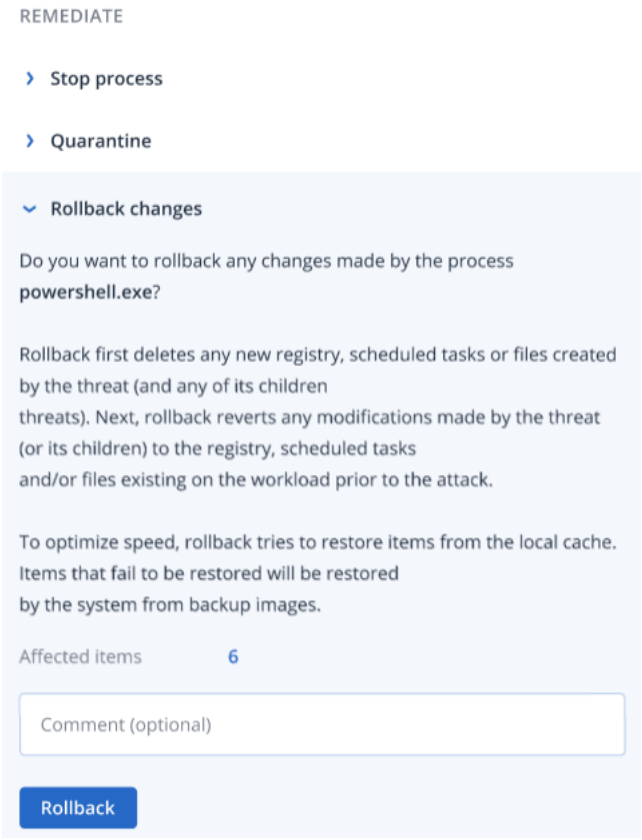
1. W cybernetycznym łańcuchu zabijania kliknij węzeł procesu, w którego przypadku chcesz wycofać zmiany.

Uwaga
Ta czynność jest dostępna tylko w przypadku węzłów wykrycia (oznaczonych kolorem czerwonym lub żółtym).

2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.

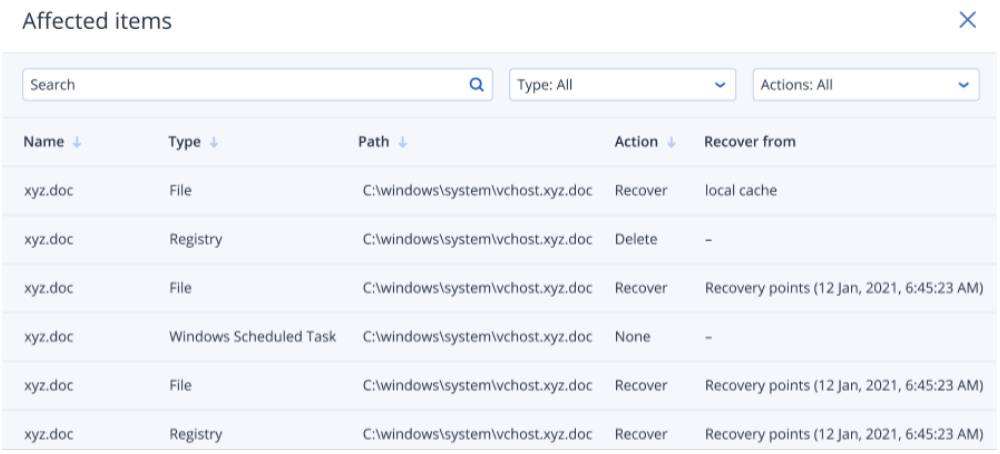
© Acronis International GmbH, 2003-2024

3. W sekcji **Napraw** kliknij **Wycofaj zmiany**.



Uwaga
Proces wycofywania odzyskuje dane wyłącznie z elementów bufora lokalnego. Wycofywanie z archiwów kopii zapasowych będzie dostępne w przyszłych wersjach.

4. Aby wyświetlić elementy, których dotyczy wycofanie zmian, kliknij łącze **Elementy, których dotyczy problem**. W wyświetlonym oknie dialogowym zostaną wyświetlone wszystkie elementy przywracane w ramach wycofywania (pliki, rejestr, zaplanowane zadania) oraz zastosowane do nich czynności (**Usuń**, **Odzyskaj** lub **Brak**). Będzie też widać, czy przywracane elementy zostaną odzyskane z lokalnej pamięci podręcznej, czy z punktów odzyskiwania kopii zapasowej.



© Acronis International GmbH, 2003-2024

5. [Opcjonalnie] Dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
6. Kliknij **Wycofaj**. Funkcja wycofywania odwraca wszelkie zmiany wprowadzone przez proces w rejestrze, plikach lub zaplanowanych zadaniach w następujących krokach:
   a. Zostaną usunięte wszystkie nowe wpisy (rejestr, zaplanowane zadania lub pliki) utworzone przez dane zagrożenie (i jego zagrożenia podrzędne).
   b. Zostaną cofnięte wszelkie modyfikacje dokonane przez zagrożenie (i jego zagrożenia podrzędne) w rejestrze, zaplanowanych zadaniach i/lub plikach istniejących na obciążeniu przed atakiem.
   c. W ramach wycofywania zostanie podjęta próba odzyskania elementów z lokalnej pamięci podręcznej. W przypadku elementów, których nie można odzyskać, moduł EDR automatycznie odzyska je z czystych obrazów kopii zapasowych.

   Czynność wycofywania będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

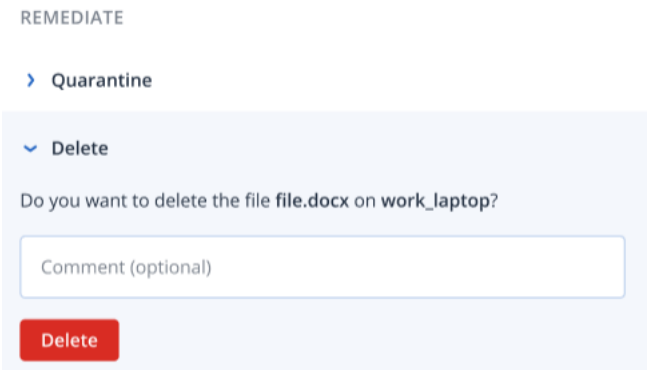
Definiowanie czynności w ramach reagowania dotyczących podejrzanego pliku

W ramach działań naprawczych podejmowanych w reakcji na atak możesz wykonać następujące czynności w odniesieniu do podejrzanych plików:

- Usunięcie pliku (zobacz niżej)
- Poddanie pliku kwarantannie (zobacz niżej)
- Dodanie pliku do listy dozwolonych lub zablokowanych w planie ochrony (zobacz "Dodawanie lub usuwanie procesu, pliku bądź sieci na liście zablokowanych lub dozwolonych planu ochrony" (s. 1027))

Aby usunąć podejrzany plik

1. W cybernetycznym łańcuchu zabijania kliknij węzeł pliku, który chcesz naprawić.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Napraw** kliknij **Usuń**.

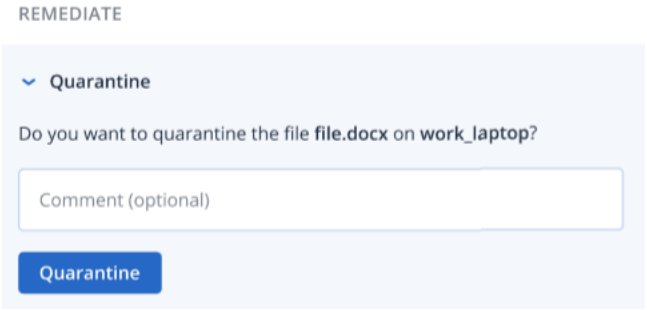


© Acronis International GmbH, 2003-2024

4. [Opcjonalnie] Dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
5. Kliknij **Usuń**.
   Plik zostanie usunięty. Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Aby poddać podejrzany plik kwarantannie

1. W cybernetycznym łańcuchu zabijania kliknij węzeł pliku, który chcesz naprawić.
2. Na wyświetlonym pasku bocznym przejdź do karty **Czynności w ramach reagowania**.
3. W sekcji **Napraw** kliknij **Kwarantanna**.



4. [Opcjonalnie] Dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
5. Kliknij **Kwarantanna**.
   Plik zostanie poddany kwarantannie. Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Definiowanie czynności w ramach reagowania dotyczących podejrzanego wpisu rejestru

W ramach działań naprawczych podejmowanych w reakcji na atak możesz usunąć podejrzane wpisy rejestru.

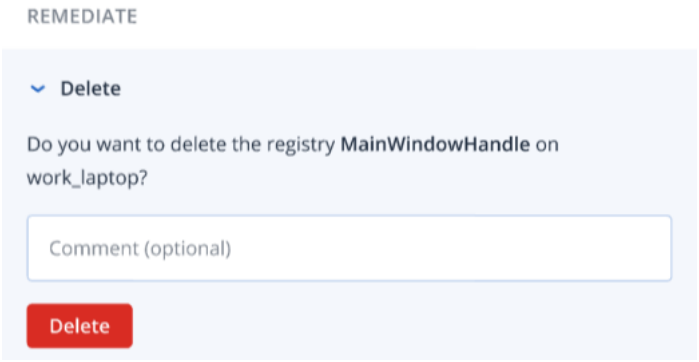
Ta opcja jest dostępna w przypadku węzłów rejestrów w cybernetycznym łańcuchu zabijania.

Aby usunąć podejrzany wpis rejestru

1. W cybernetycznym łańcuchu zabijania kliknij węzeł, który chcesz naprawić.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.

© Acronis International GmbH, 2003-2024

3. W sekcji **Napraw** kliknij **Usuń**.



4. [Opcjonalnie] Dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
5. Kliknij **Usuń**.
   Wpis rejestru zostanie usunięty. Czynność ta będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Dodawanie lub usuwanie procesu, pliku bądź sieci na liście zablokowanych lub dozwolonych planu ochrony

W ramach prewencyjnego reagowania na atak możesz dodać węzeł do listy dozwolonych lub listy zablokowanych w planie ochrony.

Możesz dodać węzeł do listy dozwolonych, jeśli uważasz, że jest on bezpieczny, i chcesz zapobiec jego wykrywaniu w przyszłości. Dodaj węzeł do listy zablokowanych, aby zapobiec jego uruchamianiu w przyszłości.

Możesz także usunąć węzeł z listy dozwolonych lub zablokowanych, aby zezwolić w przyszłości na dostęp do węzła lub go uniemożliwić.

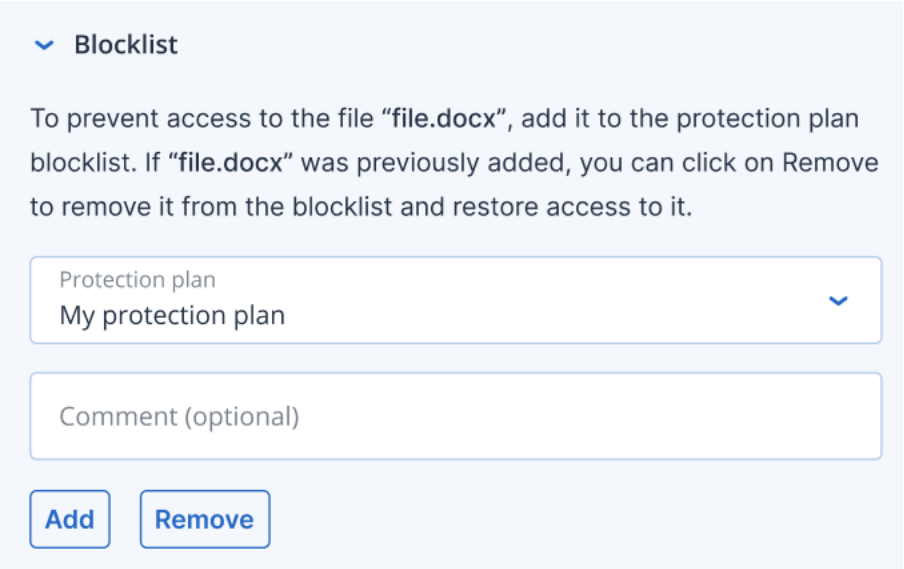
Ta opcja jest dostępna w przypadku następujących węzłów w cybernetycznym łańcuchu zabijania (Cyber Kill Chain):

- Proces
- Plik
- Sieć

Aby dodać lub usunąć proces, plik bądź sieć na liście zablokowanych planu ochrony

1. W cybernetycznym łańcuchu zabijania kliknij węzeł procesu, pliku lub sieci, który chcesz naprawić.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Zapobiegaj** kliknij ikonę strzałki obok pozycji **Lista zablokowanych**.

© Acronis International GmbH, 2003-2024

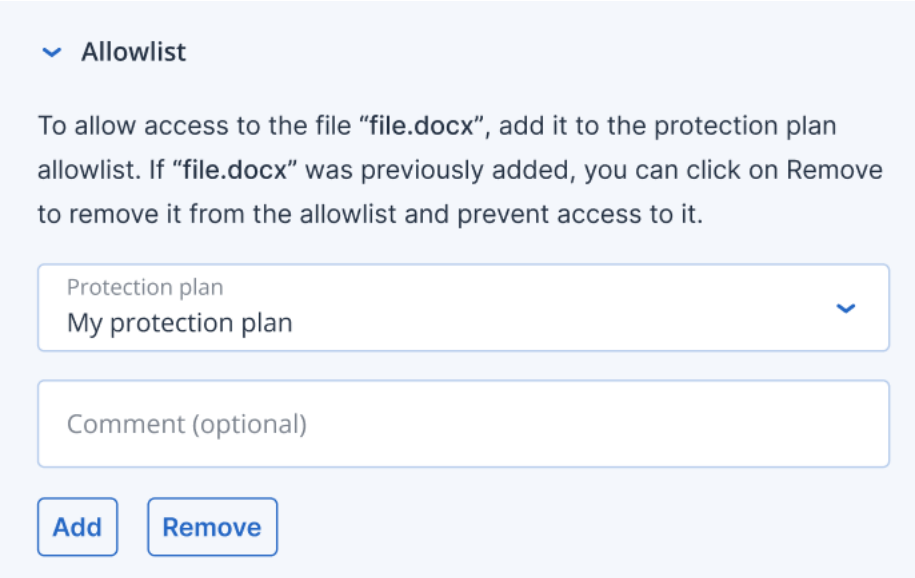


4. Wybierz plany ochrony, do których chcesz zastosować tę czynność.
5. [Opcjonalnie] Dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
6. Kliknij **Dodaj**.
   Czynność zostanie wykonana i w przyszłości nie będzie już można uruchomić danego procesu, pliku lub sieci.
   Ewentualnie, jeśli proces, plik lub sieć zostały wcześniej dodane do listy zablokowanych, a teraz chcesz je usunąć z tej listy, kliknij **Usuń**. Umożliwi to w przyszłości dostęp do węzła.
   Czynność dodania lub usunięcia będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz sekcję "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Aby dodać lub usunąć proces, plik bądź sieć na liście dozwolonych planu ochrony

1. W cybernetycznym łańcuchu zabijania kliknij węzeł procesu, pliku lub sieci, który chcesz naprawić.
2. Na wyświetlonym pasku bocznym kliknij kartę **Czynności w ramach reagowania**.
3. W sekcji **Zapobiegaj** kliknij ikonę strzałki obok pozycji **Lista dozwolonych**.

© Acronis International GmbH, 2003-2024



4. Wybierz plany ochrony, do których chcesz zastosować tę czynność.
5. [Opcjonalnie] Dodaj komentarz. Komentarz ten będzie widoczny na karcie **Działania** (dla jednego węzła lub całego incydentu) i przypomni Ci (lub Twoim współpracownikom) powody wykonania danej czynności, gdy po jakimś wrócisz do tego incydentu.
6. Kliknij **Dodaj**.
   Czynność zostanie wykonana i w przyszłości nie będzie już można wykryć danego procesu, pliku lub sieci.
   Ewentualnie, jeśli proces, plik lub sieć zostały wcześniej dodane do listy dozwolonych, a teraz chcesz je usunąć z tej listy, kliknij **Usuń**. Uniemożliwi to w przyszłości dostęp do węzła.
   Czynność dodania lub usunięcia będzie też widoczna na kartach **Działania** w przypadku zarówno węzła, jak i całego incydentu. Aby uzyskać więcej informacji, zobacz sekcję "Poznawanie czynności podjętych w celu zniwelowania skutków incydentu" (s. 995).

Włączanie trybu monitorowania dla modułu Endpoint Detection and Response (EDR)

Tryb monitorowania dostępny w oprogramowaniu Cyber Protection umożliwia korzystanie z funkcji EDR w środowisku produkcyjnym. To z kolei umożliwia sprawdzenie, czy występują jakiekolwiek fałszywe alarmy, i dokonanie niezbędnych wykluczeń przed pełnym wdrożeniem EDR.

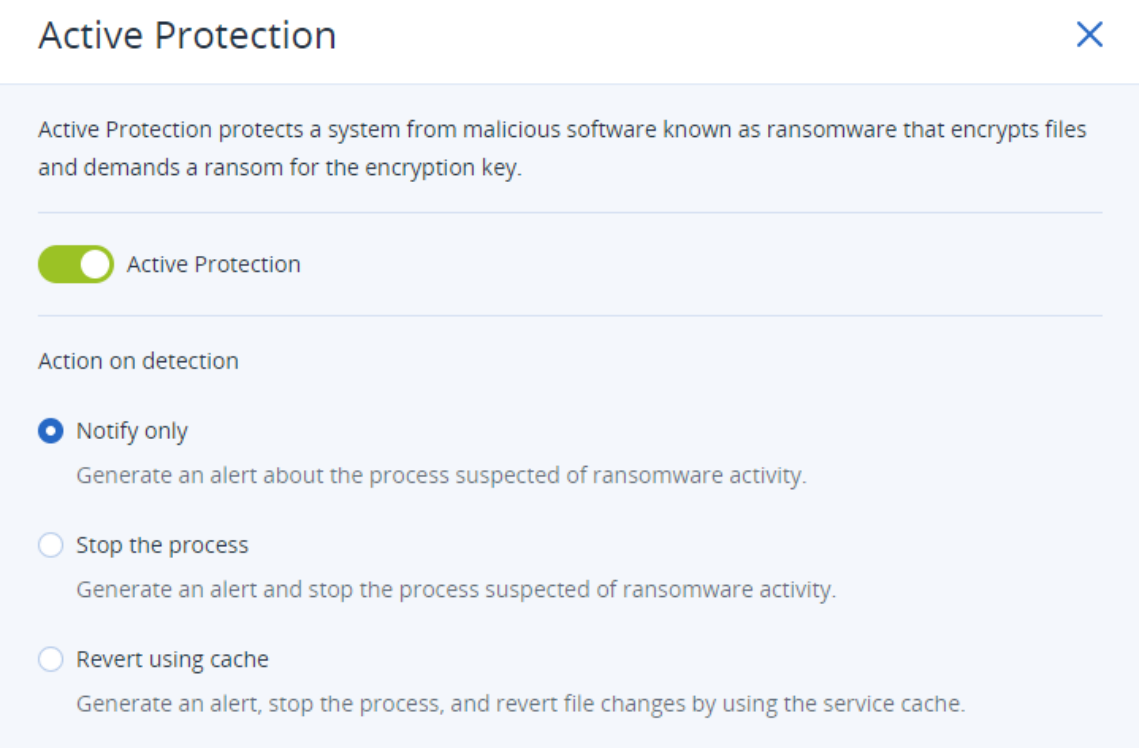
W trybie monitorowania nic nie jest blokowane ani zatrzymywane. Incydenty są tworzone, ale nie są inicjowane żadne czynności w ramach reagowania.

Aby włączyć tryb monitorowania dla modułu EDR

1. W odpowiednim planie ochrony upewnij się, że jest włączony moduł EDR. Aby uzyskać więcej informacji, zobacz "Włączanie funkcji modułu Endpoint Detection and Response (EDR)" (s. 961).
2. Rozwiń moduł **Ochrona przed wirusami i złośliwym oprogramowaniem**, a następnie zdefiniuj następujące opcje:

© Acronis International GmbH, 2003-2024

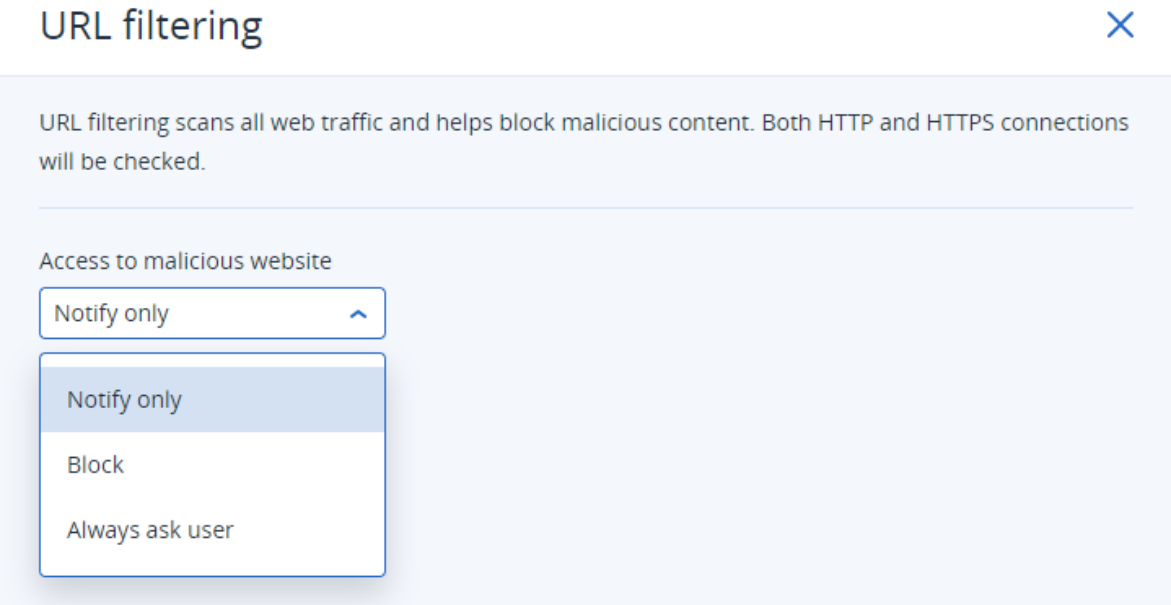
- Kliknij **Active Protection** i w sekcji **Działanie po wykryciu** wybierz **Tylko powiadom**. Następnie kliknij **Gotowe**. Aby uzyskać więcej informacji, zobacz "Active Protection" (s. 882).



- Kliknij **Mechanizm zachowań** i w sekcji **Działanie po wykryciu** wybierz **Tylko powiadom**. Następnie kliknij **Gotowe**. Aby uzyskać więcej informacji, zobacz "Mechanizm zachowań" (s. 887).
- Kliknij **Ochrona przed exploitami** i w sekcji **Działanie po wykryciu** wybierz **Tylko powiadom**. Następnie kliknij **Gotowe**. Aby uzyskać więcej informacji, zobacz "Ochrona przed exploitami" (s. 887).
- Kliknij **Ochrona w czasie rzeczywistym** i w sekcji **Działanie po wykryciu**, wybierz **Tylko powiadom**. Następnie kliknij **Gotowe**. Aby uzyskać więcej informacji, zobacz "Ochrona w czasie rzeczywistym" (s. 889).
- Kliknij **Zaplanuj skanowanie** i w sekcji **Działanie po wykryciu** wybierz **Tylko powiadom**. Następnie kliknij **Gotowe**. Aby uzyskać więcej informacji, zobacz "Zaplanuj skanowanie" (s. 890).

3. Rozwiń moduł **Filtrowanie adresów URL** i na liście rozwijanej **Dostęp do złośliwej witryny internetowej** wybierz **Tylko powiadom**. Następnie kliknij **Gotowe**. Aby uzyskać więcej informacji, zobacz "Filtrowanie adresów URL" (s. 906).

© Acronis International GmbH, 2003-2024



Sprawdzanie, czy pakiet Endpoint Detection and Response (EDR) poprawnie działa

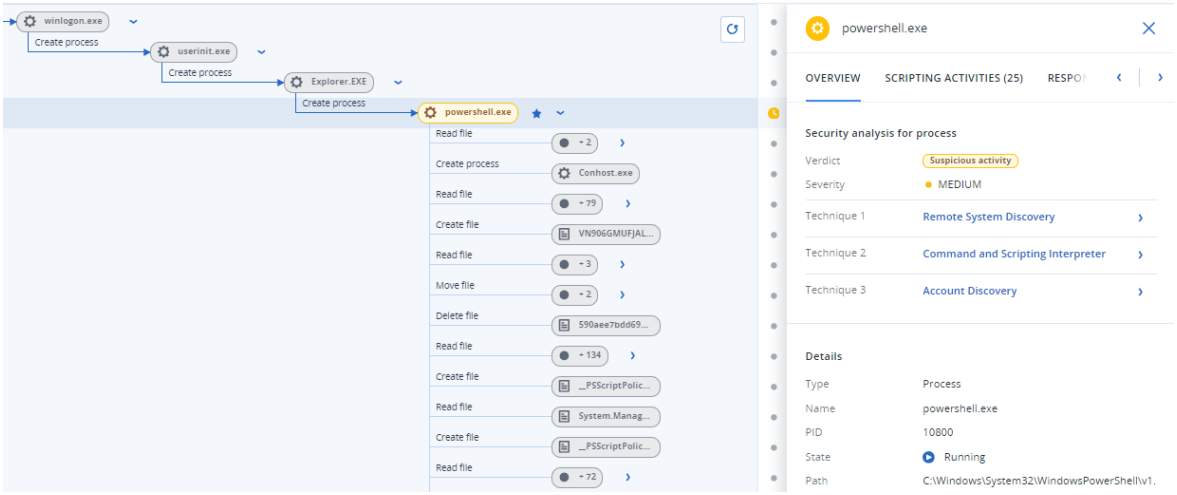
Aby się upewnić, czy pakiet EDR jest wdrożony i działa, można uruchomić szereg poleceń, które wyzwalają wykrywanie EDR.

Uwaga
Po wdrożeniu pakietu EDR każda podejrzana aktywność powinna skutkować niezwłocznym wyświetleniem incydentu. Jeśli przez kilka dni z rzędu nie zostały wyzwolone żadne incydenty, można skorzystać z poniższych instrukcji, aby sprawdzić, czy wykrywanie EDR jeszcze działa.

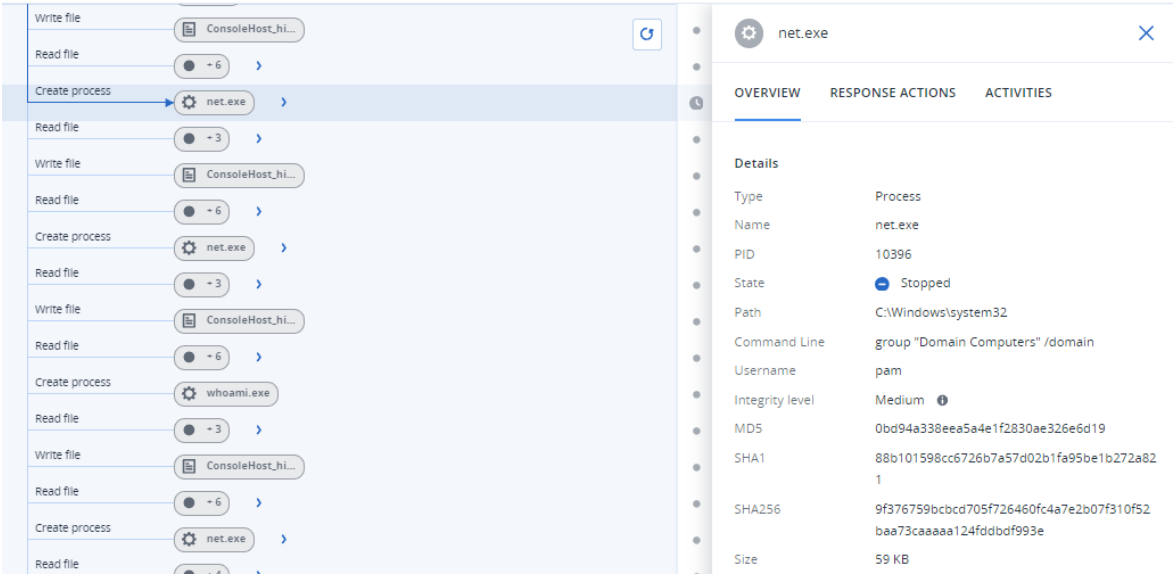
Aby sprawdzić, czy pakiet EDR jest wdrożony i poprawnie działa

1. Zaloguj się na odpowiednim połączonym z domeną koncie użytkownika usługi Active Directory.
2. W środowisku Windows PowerShell uruchom następujące dwa polecenia:
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. W konsoli Cyber Protect przejdź do sekcji **Ochrona > Incydenty**, aby wyświetlić wygenerowany incydent.
   Możesz też kliknąć wyzwolony incydent o ważności **Średnia**, aby go wyświetlić w cybernetycznym łańcuchu zabijania pakietu EDR i potwierdzić polecenia wykonywane w poprzednim kroku w środowisku PowerShell — tak jak pokazano w poniższym przykładzie.

© Acronis International GmbH, 2003-2024



4. W środowisku Windows PowerShell uruchom następujące polecenia:
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. W cybernetycznym łańcuchu zabijania pakietu EDR kliknij wykonywalne węzły (na przykład **net.exe** lub **whoami.exe**), aby wyświetlić dokładne polecenia PowerShell wykonywane w wierszu polecenia. W poniższym przykładzie polecenia te są wyświetlane w sekcji **Szczegóły** karty **Przegląd**.



6. Po potwierdzeniu wygenerowania incydentu EDR należy ręcznie ustawić opcję **Status zagrożeń** dla incydentu na **Zniwelowano** oraz opcję **Stan dochodzenia** na **Zamknięto**. Aby uzyskać więcej informacji, zobacz "Jak poddać incydenty dochodzeniu w cybernetycznym łańcuchu zabijania" (s. 986). Możesz też wprowadzić komentarz do incydentu, aby zaznaczyć, że był to

© Acronis International GmbH, 2003-2024

incydent testowy.

© Acronis International GmbH, 2003-2024

Ocena luk w zabezpieczeniach i zarządzanie poprawkami

Ocena luk w zabezpieczeniach to proces identyfikacji, szacowania ilościowego i ustalania priorytetów luk w zabezpieczeniach znalezionych w systemie. Moduł Ocena luk w zabezpieczeniach umożliwia skanowanie komputerów w poszukiwaniu luk w zabezpieczeniach, a także sprawdzanie, czy systemy operacyjne oraz zainstalowane aplikacje są aktualne i prawidłowo działają.

Skanowanie w ramach oceny luk w zabezpieczeniach jest obsługiwane w przypadku komputerów z następującymi systemami operacyjnymi:

- Windows. Aby uzyskać więcej informacji, zobacz "Obsługiwane produkty firmy Microsoft i innych firm" (s. 1035).
- macOS. Aby uzyskać więcej informacji, zobacz "Obsługiwane produkty firmy Apple i innych firm" (s. 1036).
- Komputery z systemem Linux (CentOS 7 / Virtuozzo / Acronis Cyber Infrastructure). Aby uzyskać więcej informacji, zobacz "Obsługiwane produkty dla systemu Linux" (s. 1037).

Funkcja **Zarządzanie poprawkami** umożliwia zarządzanie poprawkami (aktualizacjami) aplikacji i systemów operacyjnych zainstalowanych na komputerach oraz dbanie o ich aktualność. Moduł Zarządzanie poprawkami pozwala na automatyczne lub ręczne zatwierdzanie instalacji aktualizacji na komputerach.

Zarządzanie poprawkami jest obsługiwane w przypadku komputerów z systemami operacyjnymi Windows. Aby uzyskać więcej informacji, zobacz "Obsługiwane produkty firmy Microsoft i innych firm" (s. 1035).

Ocena luk w zabezpieczeniach

Proces oceny luk w zabezpieczeniach obejmuje następujące etapy:

1. Ty tworzysz plan ochrony z włączonym modułem Ocena luk w zabezpieczeniach, określasz ustawienia oceny luk w zabezpieczeniach i przypisujesz plan do komputerów.
2. System — według harmonogramu lub na żądanie — wysyła do zainstalowanych na komputerach agentów ochrony polecenie uruchomienia skanowania w celu oceny luk w zabezpieczeniach.
3. Agenty otrzymują polecenie, uruchamiają mechanizmy skanowania w poszukiwaniu luk w zabezpieczeniach i podejmują działania związane ze skanowaniem.
4. Po zakończeniu skanowania agenty generują wyniki i wysyłają je do usługi monitorowania.
5. Usługa monitorowania przetwarza dane od agentów i wyświetla wyniki w widżetach oceny luk w zabezpieczeniach oraz na liście znalezionych luk.
6. Po uzyskaniu listy znalezionych luk w zabezpieczeniach możesz ją przeanalizować i zdecydować, które luki w zabezpieczeniach muszą zostać usunięte.

Wyniki skanowania w celu oceny luk w zabezpieczeniach można monitorować w widżetach **Monitorowanie** > **Przegląd** > **Luki w zabezpieczeniach / Występujące luki w zabezpieczeniach**.

© Acronis International GmbH, 2003-2024

Obsługiwane produkty firmy Microsoft i innych firm

Ocena luk w zabezpieczeniach i zarządzanie poprawkami są obsługiwane w przypadku następujących produktów firmy Microsoft i innych firm przeznaczonych do systemów operacyjnych Windows:

Obsługiwane produkty firmy Microsoft

Windows OS

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server OS

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office i związane z nim komponenty

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Komponenty związane z systemem Windows OS

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio i aplikacje
- Komponenty systemu operacyjnego

Aplikacje serwerowe

© Acronis International GmbH, 2003-2024

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Obsługiwane produkty innych firm przeznaczone do systemu operacyjnego Windows

Praca zdalna jest coraz bardziej powszechna na całym świecie, dlatego jest to bardzo ważne, aby narzędzia do współpracy i komunikacji oraz klienty VPN były zawsze aktualne i sprawdzane pod kątem ewentualnych luk w zabezpieczeniach. Usługa Cyber Protection obsługuje oceny luk w zabezpieczeniach i zarządzanie poprawkami w przypadku takich aplikacji.

Narzędzia do współpracy i komunikacji, klienty VPN

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Więcej informacji o obsługiwanych produktach innych firm przeznaczonych do systemu operacyjnego Windows można znaleźć w artykule Lista produktów innych firm obsługiwanych przez usługę Zarządzanie poprawkami (62853).

Obsługiwane produkty firmy Apple i innych firm

Ocena luk w zabezpieczeniach jest obsługiwana w przypadku następujących produktów firmy Apple i innych firm dla systemu macOS:

Obsługiwane produkty firmy Apple

macOS

© Acronis International GmbH, 2003-2024

- macOS 10.13.x lub nowszy

Wbudowane aplikacje systemu macOS

- Safari, iTunes i inne

Obsługiwane produkty innych firm dla systemu macOS

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC media player

Obsługiwane produkty dla systemu Linux

Ocena luk w zabezpieczeniach jest obsługiwana w przypadku następujących dystrybucji i wersji systemu Linux:

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Ustawienia modułu Ocena luk w zabezpieczeniach

Więcej informacji na temat tworzenia planu ochrony z wykorzystaniem modułu Ocena luk w zabezpieczeniach można znaleźć w sekcji „Tworzenie planu ochrony”. Skanowanie w celu oceny luk w zabezpieczeniach można przeprowadzać według harmonogramu lub na żądanie (przy użyciu czynności **Uruchom teraz** w planie ochrony).

W module Ocena luk w zabezpieczeniach można określić następujące ustawienia:

Elementy do skanowania

Wybierz oprogramowanie, które chcesz przeskanować pod kątem luk w zabezpieczeniach:

- Komputery z systemem Windows:
  - **Produkty firmy Microsoft**
  - **Produkty innych firm przeznaczone do systemu Windows** (Więcej informacji o obsługiwanych produktach innych firm przeznaczonych do systemu operacyjnego Windows

© Acronis International GmbH, 2003-2024

można znaleźć w artykule Lista produktów innych firm obsługiwanych przez usługę Zarządzanie poprawkami (62853)).

- Komputery z systemem macOS:
  - **Produkty firmy Apple**
  - **Produkty innych firm przeznaczone do systemu macOS**
- Komputery z systemem Linux:
  - **Skanuj pakiety systemu Linux**

Harmonogram

Zdefiniuj harmonogram, zgodnie z którym na wybranych komputerach ma być wykonywane skanowanie w celu oceny luk w zabezpieczeniach:

Pole	Opis
Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń	To ustawienie umożliwia określenie czasu uruchomienia zadania. Dostępne są następujące wartości: • **Zaplanuj według czasu** — jest to ustawienie domyślne. Zadanie zostanie uruchomione w określonym czasie. • **Gdy użytkownik zaloguje się w systemie** — domyślnie zalogowanie się dowolnego użytkownika spowoduje wyzwolenie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika. • **Gdy użytkownik wyloguje się z systemu** — domyślnie wylogowanie się dowolnego użytkownika spowoduje wyzwolenie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika. **Uwaga** Zadanie nie zostanie uruchomione przy zamykaniu systemu. Zamknięcie systemu i wylogowanie to różne zdarzenia w konfiguracji harmonogramu. • **Podczas uruchamiania systemu** — zadanie zostanie uruchomione podczas uruchamiania systemu operacyjnego. • **Podczas zamknięcia systemu** — zadanie zostanie uruchomione podczas zamykania systemu operacyjnego.
Typ harmonogramu	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Dostępne są następujące wartości: • **Co miesiąc** — należy wybrać miesiące i tygodnie lub dni miesiąca, w których zadanie będzie uruchamiane.

© Acronis International GmbH, 2003-2024

Pole	Opis
	• **Codziennie** — jest to ustawienie domyślne. Wybierz dni tygodnia, w które będzie uruchamiane zadanie. • **Co godzinę** — należy wybrać dni tygodnia, liczbę powtórzeń oraz przedział czasu, w których zadanie będzie uruchamiane.
Czas rozpoczęcia	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu** Wybierz dokładną godzinę, o której zostanie uruchomione zadanie.
Uruchom w podanym okresie	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Ustaw zakres czasu, w którym będzie obowiązywać skonfigurowany harmonogram.
Określ konto użytkownika, którego zalogowanie się w systemie operacyjnym zainicjuje wykonanie zadania	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Gdy użytkownik zaloguje się w systemie**. Dostępne są następujące wartości: • **Dowolny użytkownik** — użyj tej opcji, jeśli chcesz, aby zalogowanie się dowolnego użytkownika powodowało wyzwolenie zadania. • **Następujący użytkownik** — użyj tej opcji, jeśli chcesz, aby tylko zalogowanie się na określonym koncie użytkownika powodowało wyzwolenie zadania.
Określ konto użytkownika, którego wylogowanie się z systemu operacyjnego zainicjuje wykonanie zadania	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Gdy użytkownik wyloguje się z systemu**. Dostępne są następujące wartości: • **Dowolny użytkownik** — użyj tej opcji, jeśli chcesz, aby wylogowanie się dowolnego użytkownika powodowało wyzwolenie zadania. • **Następujący użytkownik** — użyj tej opcji, jeśli chcesz, aby tylko wylogowanie się z określonego konta użytkownika powodowało wyzwolenie zadania.
Warunki rozpoczęcia	Określ wszystkie warunki, które muszą być jednocześnie spełnione, aby zostało uruchomione zadanie. Warunki rozpoczęcia skanowania pod kątem złośliwego oprogramowania są podobne do warunków uruchomienia modułu **Kopia zapasowa**, które opisano w sekcji „Warunki rozpoczęcia”. Można zdefiniować następujące dodatkowe warunki uruchomienia:

© Acronis International GmbH, 2003-2024

Pole	Opis
	• **Rozłóż rozpoczęcie zadania w przedziale czasu** — ta opcja umożliwia zdefiniowanie ram czasowych zadań, aby uniknąć wąskich gardeł na łączach sieciowych. Możesz określić opóźnienie w godzinach lub minutach. Jeśli na przykład domyślną godziną rozpoczęcia jest 10:00, a opóźnienie wynosi 60 minut, to zadanie rozpocznie się między godziną 10:00 a 11:00. • **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu** • **Zablokuj włączanie trybu uśpienia lub hibernacji podczas wykonywania zadania** — ta opcja działa tylko w przypadku komputerów z systemem Windows. • **Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie po** — określ czas, po którym zadanie zostanie uruchomione, bez względu na spełnienie innych warunków rozpoczęcia. **Uwaga** Warunki uruchomienia nie są obsługiwane w systemie Linux.

Ocena luk w zabezpieczeniach komputerów z systemem Windows

Komputery z systemem Windows i produktami innych firm dla systemu Windows można skanować w poszukiwaniu luk w zabezpieczeniach.

Aby skonfigurować ocenę luk w zabezpieczeniach komputerów z systemem Windows

1. W konsoli Cyber Protect utwórz plan ochrony i włącz moduł **Ocena luk w zabezpieczeniach**.
2. Określ ustawienia oceny luk w zabezpieczeniach:
   - **Elementy do skanowania** — zaznacz **Produkty firmy Microsoft**, **Produkty firmy Microsoft, produkty innych firm przeznaczone do systemu Windows** lub obie te opcje.
   - **Harmonogram** — określ harmonogram przeprowadzania ocen luk w zabezpieczeniach.

   Dodatkowe informacje na temat opcji **Harmonogram** można znaleźć w sekcji "Ustawienia modułu Ocena luk w zabezpieczeniach" (s. 1037).
3. Przypisz plan do komputerów z systemem Windows.

Po przeprowadzeniu skanowania w celu oceny luk w zabezpieczeniach możesz sprawdzić listę znalezionych luk. Możesz przeanalizować te informacje i zdecydować, które luki w zabezpieczeniach muszą zostać usunięte.

Aby monitorować wyniki skanowania w celu oceny luk w zabezpieczeniach, skorzystaj z widżetów **Monitorowanie** > **Przegląd** > **Luki w zabezpieczeniach / Występujące luki w zabezpieczeniach**.

© Acronis International GmbH, 2003-2024

Ocena luk w zabezpieczeniach w przypadku komputerów z systemem Linux

Możesz skanować komputery z systemem Linux w poszukiwaniu luk w zabezpieczeniach na poziomie aplikacji i jądra.

Aby skonfigurować ocenę luk w zabezpieczeniach w przypadku komputerów z systemem Linux

1. W konsoli Cyber Protect utwórz plan ochrony i włącz moduł **Ocena luk w zabezpieczeniach**.
2. Określ ustawienia oceny luk w zabezpieczeniach:
   - **Elementy do skanowania** — wybierz **Skanuj pakiety systemu Linux**.
   - **Harmonogram** — określ harmonogram przeprowadzania ocen luk w zabezpieczeniach.

   Dodatkowe informacje na temat opcji **Harmonogram** można znaleźć w sekcji "Ustawienia modułu Ocena luk w zabezpieczeniach" (s. 1037).
3. Przypisz plan do komputerów z systemem Linux.

Po przeprowadzeniu skanowania w celu oceny luk w zabezpieczeniach możesz sprawdzić listę znalezionych luk. Możesz przeanalizować te informacje i zdecydować, które luki w zabezpieczeniach muszą zostać usunięte.

Aby monitorować wyniki skanowania w celu oceny luk w zabezpieczeniach, skorzystaj z widżetów **Monitorowanie** > **Przegląd** > **Luki w zabezpieczeniach / Występujące luki w zabezpieczeniach**.

Ocena luk w zabezpieczeniach urządzeń z systemem macOS

Urządzenia z systemem macOS można skanować pod kątem luk w zabezpieczeniach na poziomie systemu operacyjnego i aplikacji.

Aby skonfigurować ocenę luk w zabezpieczeniach urządzeń z systemem macOS

1. W konsoli Cyber Protect utwórz plan ochrony i włącz moduł **Ocena luk w zabezpieczeniach**.
2. Określ ustawienia oceny luk w zabezpieczeniach:
   - **Elementy do skanowania** — zaznacz **Produkty firmy Apple**, **Produkty innych firm przeznaczone do systemu macOS** lub obie te opcje.
   - **Harmonogram** — określ harmonogram przeprowadzania ocen luk w zabezpieczeniach.

   Dodatkowe informacje na temat opcji **Harmonogram** można znaleźć w sekcji "Ustawienia modułu Ocena luk w zabezpieczeniach" (s. 1037).
3. Przypisz plan do urządzeń z systemem macOS.

Po przeprowadzeniu skanowania w celu oceny luk w zabezpieczeniach możesz sprawdzić listę znalezionych luk. Możesz przeanalizować te informacje i zdecydować, które luki w zabezpieczeniach muszą zostać usunięte.

Aby monitorować wyniki skanowania w celu oceny luk w zabezpieczeniach, skorzystaj z widżetów **Monitorowanie** > **Przegląd** > **Luki w zabezpieczeniach / Występujące luki w zabezpieczeniach**.

© Acronis International GmbH, 2003-2024

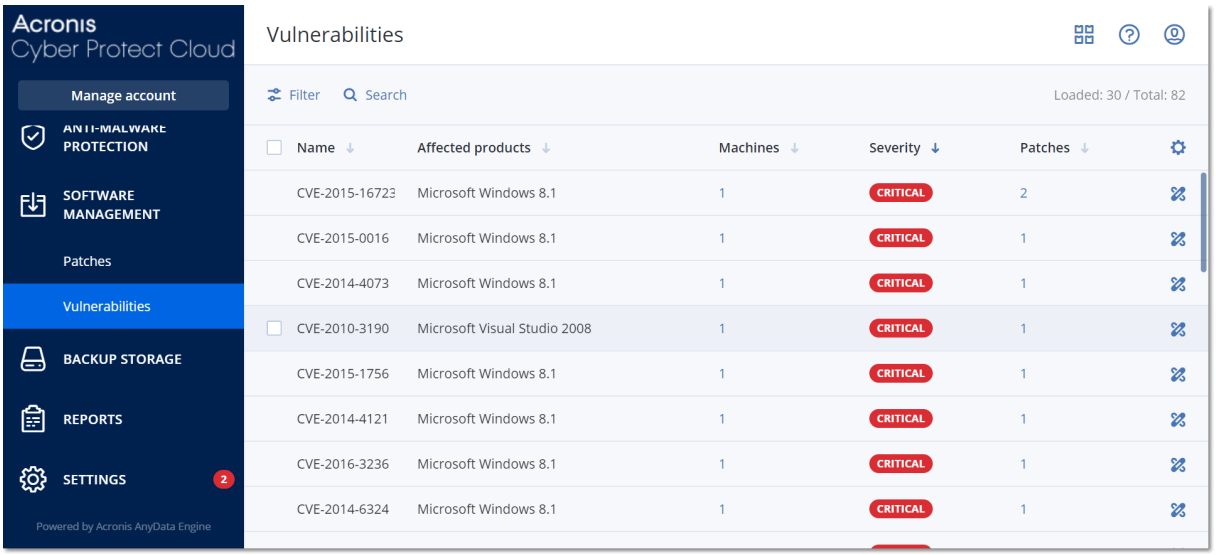
Zarządzanie znalezionymi lukami w zabezpieczeniach

Jeśli choć raz wykonano ocenę luk w zabezpieczeniach i wykryto jakieś luki, będą one widoczne w sekcji **Zarządzanie oprogramowaniem** > **Luki w zabezpieczeniach**. Na liście luk w zabezpieczeniach są pokazywane zarówno luki, w których przypadku są dostępne poprawki do zainstalowania, jak i te, dla których nie ma proponowanych poprawek. Korzystając z filtru, można wyświetlić tylko luki z poprawkami.

Nazwa	Opis
Nazwa	Nazwa luki w zabezpieczeniach.
Produkty dotknięte problemem	Programy, w których wykryto luki.
Komputery	Liczba komputerów dotkniętych problemem.
Ważność	Ważność znalezionej luki. Może to być jeden z następujących poziomów ważności określony zgodnie z systemem Common Vulnerability Scoring System (CVSS): • **Krytyczne**: 9–10 w skali CVSS • **Wysoki**: 7–9 w skali CVSS • **Średni**: 3–7 w skali CVSS • **Niski**: 0–3 w skali CVSS • **Brak**
Poprawki	Liczba odpowiednich poprawek.
Opublikowano	Data i godzina opublikowania luki w zabezpieczeniach na liście Common Vulnerabilities and Exposures (CVE).
Wykryto	Dzień pierwszego wykrycia danej luki na komputerach.

Opis znalezionej luki w zabezpieczeniach można wyświetlić przez kliknięcie jej nazwy na liście.

© Acronis International GmbH, 2003-2024



Aby rozpocząć naprawianie luk w zabezpieczeniach

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Luki w zabezpieczeniach**.
2. Wybierz lukę z listy, a następnie kliknij **Zainstaluj poprawki**. Zostanie otwarty kreator naprawy luk w zabezpieczeniach.
3. Wybierz poprawki do zainstalowania na wybranych komputerach, a następnie kliknij **Dalej**.
4. Wybierz komputery, na których chcesz zainstalować poprawki.
5. Wybierz opcje ponownego uruchomienia.
   a. Wybierz, czy komputer ma zostać uruchomiony ponownie po zainstalowaniu poprawek.

Opcja	Opis
Nie	Komputery nie zostaną automatycznie uruchomione ponownie po zainstalowaniu poprawek.
Jeśli jest to wymagane	Komputery zostaną uruchomione ponownie tylko wtedy, gdy jest to niezbędne do zastosowania poprawek.
Tak	Komputery zostaną automatycznie uruchomione ponownie po zainstalowaniu poprawek. Można też określić opóźnienie ponownego uruchomienia.

   b. [Opcjonalnie] Jeśli chcesz opóźnić ponowne uruchomienie komputera o czas tworzenia jego kopii zapasowej, wybierz **Nie uruchamiaj ponownie, dopóki nie zakończy się tworzenie kopii zapasowej**.
6. Kliknij **Zainstaluj poprawki**.

W wyniku tego na wybranych komputerach zostaną zainstalowane wybrane poprawki.

© Acronis International GmbH, 2003-2024

Zarządzanie poprawkami

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Więcej informacji o obsługiwanych produktach innych firm przeznaczonych do systemu operacyjnego Windows można znaleźć w artykule Lista produktów innych firm obsługiwanych przez usługę Zarządzanie poprawkami (62853).

Funkcja zarządzania poprawkami umożliwia:

- instalowanie aktualizacji na poziomie aplikacji
- ręczne lub automatyczne zatwierdzanie poprawek
- instalowanie poprawek na żądanie lub zgodnie z harmonogramem
- dokładne określanie, które poprawki mają zostać zainstalowane, przy użyciu różnych kryteriów: ważność, kategoria i status zatwierdzenia
- tworzenie kopii zapasowych przed zainstalowaniem aktualizacji, aby zapobiec ewentualnym nieudanym aktualizacjom
- określanie czynności ponownego uruchomienia, która ma zostać wykonana po zainstalowaniu poprawki

Uwaga
Aby móc pracować z aktualizacjami systemu Windows, funkcja zarządzania poprawkami wymaga włączenia na maszynie aktualizacji systemu Windows.

Aby zminimalizować ruch w sieci, usługa Cyber Protection stosuje technologię komunikacji peer-to-peer. Możesz wybrać specjalne agenty, które będą pobierać aktualizacje z Internetu i je rozpowszechniać wśród innych agentów w sieci. Wszystkie agenty będą też udostępniać sobie nawzajem aktualizacje jako agenty peer-to-peer.

Przepływ pracy zarządzania poprawkami

Przepływ pracy zarządzania poprawkami obejmuje etapy konfigurowania i stosowania planu ochrony, uruchamiania skanowania w celu oceny luk w zabezpieczeniach, konfigurowania ustawień poprawek, zatwierdzania poprawek i wreszcie instalowania zatwierdzonych poprawek. Dokładne etapy tego przepływu pracy są następujące.

1. Skonfiguruj plan ochrony z włączonymi modułami **Ocena luk w zabezpieczeniach** i **Zarządzanie poprawkami**.
2. Skonfiguruj ustawienia oceny luk w zabezpieczeniach. Dodatkowe informacje na temat tych ustawień można znaleźć w sekcji "Ustawienia modułu Ocena luk w zabezpieczeniach" (s. 1037).
3. Skonfiguruj ustawienia zarządzania poprawkami. Dodatkowe informacje na temat tych ustawień można znaleźć w sekcji "Ustawienia zarządzania poprawkami w planie ochrony" (s. 1045)

© Acronis International GmbH, 2003-2024

4. Zastosuj plan ochrony do co najmniej jednego komputera.
5. Poczekaj na zakończenie skanowania w celu oceny luk w zabezpieczeniach. Skanowanie rozpocznie się automatycznie, zgodnie z harmonogramem skonfigurowanym w planie ochrony. Możesz też ręcznie uruchomić skanowanie na żądanie, klikając ikonę **Uruchom teraz** w module **Ocena luk w zabezpieczeniach** w planie ochrony.
6. Zatwierdź poprawki. Możesz zdefiniować ustawienia automatycznego zatwierdzania poprawek, które obejmują automatyczną instalację poprawek na komputerach testowych. Aby uzyskać więcej informacji, zobacz "Automatyczne zatwierdzanie poprawek" (s. 1053). Możesz też ręcznie zatwierdzać poprawki, ustawiając ich status zatwierdzenia na **Zatwierdzono**. Aby uzyskać więcej informacji, zobacz "Ręczne zatwierdzanie poprawek" (s. 1058).
7. Zainstaluj poprawki. Zatwierdzone poprawki mogą być instalowane automatycznie, zgodnie z harmonogramem skonfigurowanym w planie ochrony. Można też ręcznie instalować poprawki na żądanie. Aby uzyskać więcej informacji, zobacz "Instalowanie poprawek na żądanie" (s. 1058).

Wyniki instalacji poprawek można monitorować w widżecie **Monitorowanie** > **Przegląd** > **Historia instalacji poprawek**.

Ustawienia zarządzania poprawkami w planie ochrony

W module **Zarządzanie poprawkami** planu ochrony możesz skonfigurować następujące aspekty zarządzania poprawkami:

- Jakie aktualizacje mają zostać zainstalowane w przypadku produktów firmy Microsoft i innych firm przeznaczonych do systemu operacyjnego Windows.
- Kiedy ma zostać uruchomiona automatyczna instalacja poprawek.
- Czy przed aktualizacją ma zostać wykonana operacja tworzenia kopii zapasowej.

Dodatkowe informacje na temat tworzenia planu ochrony i włączania modułu **Zarządzanie poprawkami** można znaleźć w sekcji "Tworzenie planu ochrony" (s. 222).

Uwaga
Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Produkty firmy Microsoft

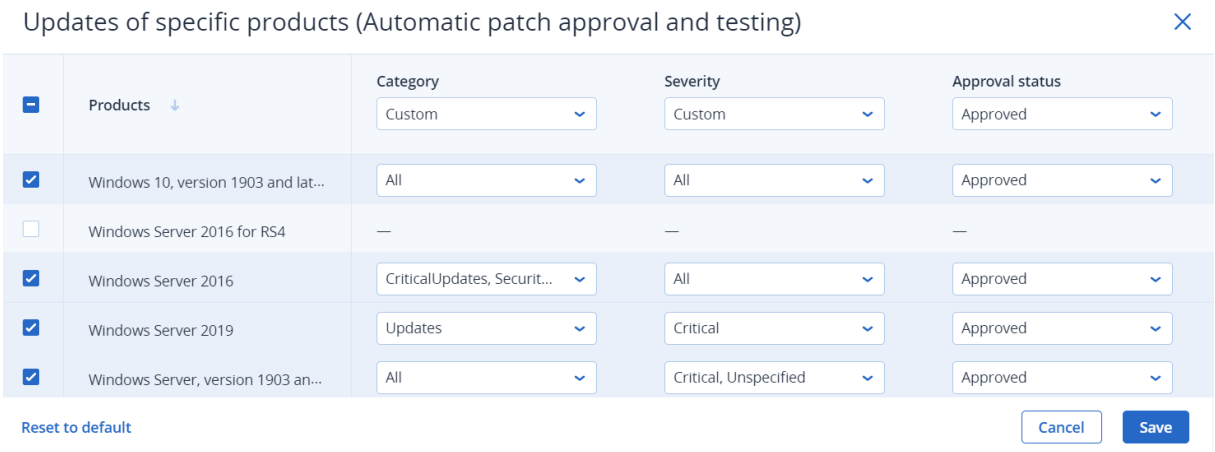
Aby zainstalować aktualizacje firmy Microsoft na wybranych komputerach, włącz opcję **Aktualizuj produkty firmy Microsoft**.

Wybierz opcję instalacji:

Opcja	Opis
Wszystkie aktualizacje	Użyj tej opcji, jeśli chcesz zainstalować wszystkie zatwierdzone aktualizacje.
Tylko aktualizacje zabezpieczeń i	Użyj tej opcji, jeśli chcesz zainstalować wszystkie aktualizacje zabezpieczeń i aktualizacje krytyczne.

© Acronis International GmbH, 2003-2024

Opcja	Opis
aktualizacje krytyczne	
Aktualizacje określonych produktów (automatyczne zatwierdzanie poprawek i testy)	Użyj tej opcji, jeśli chcesz zdefiniować niestandardowe ustawienia dla różnych produktów. Jeśli chcesz zaktualizować określone produkty, w przypadku każdego z nich możesz zdefiniować, które aktualizacje mają zostać zainstalowane, na podstawie kategorii, ważności lub statusu zatwierdzenia. Wybierz tę opcję, jeśli chcesz skonfigurować automatyczne zatwierdzanie i testy poprawek.



W przypadku produktów firmy Microsoft mechanizm dystrybucji poprawek wykorzystuje usługę Windows API. Poprawki i aktualizacje nie są pobierane i zapisywane wewnętrznie ani na agentach do dystrybucji. Zamiast tego są pobierane z usługi Microsoft CDN. Dlatego agent nie może pobierać ani dystrybuować poprawek, nawet jeśli ma przypisaną rolę Aktualizator.

Produkty innych firm przeznaczone do systemu Windows

Aby zainstalować aktualizacje produktów innych firm przeznaczonych do systemu Windows na wybranych komputerach, włącz opcję **Produkty innych firm przeznaczone do systemu Windows**.

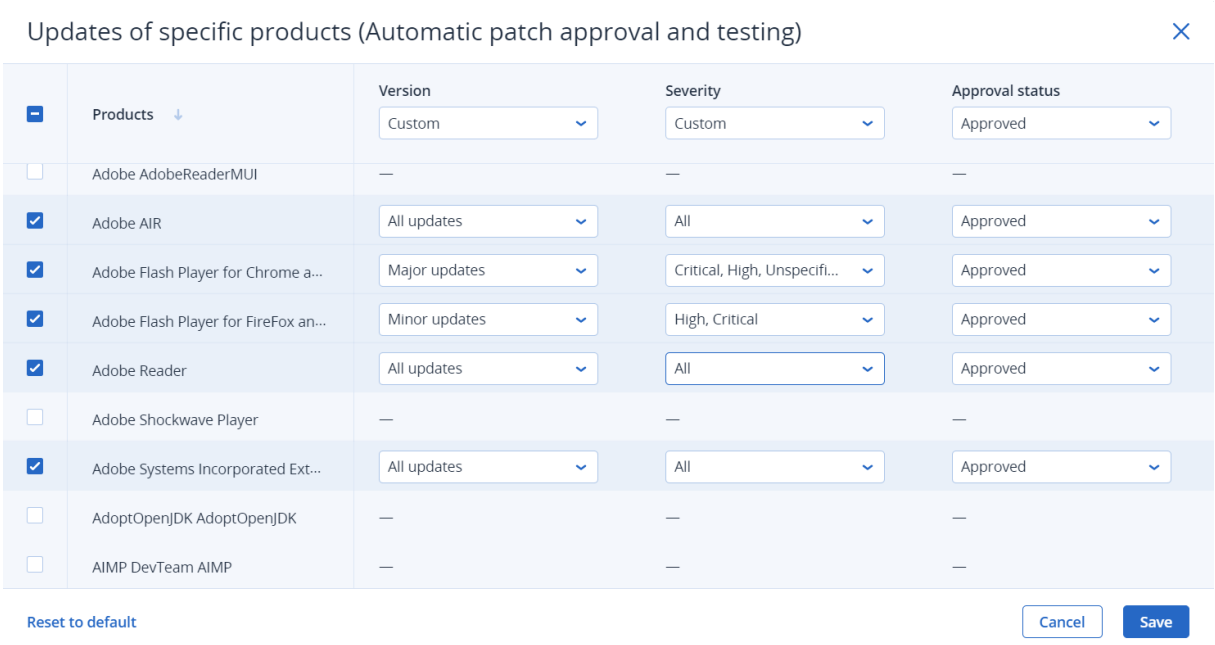
Wybierz opcje instalacji:

Opcja	Opis
Wszystkie aktualizacje	Użyj tej opcji, jeśli chcesz zainstalować wszystkie zatwierdzone aktualizacje*.
Tylko ważne aktualizacje	Użyj tej opcji, jeśli chcesz zainstalować wszystkie zatwierdzone ważne aktualizacje.
Tylko drobne aktualizacje	Użyj tej opcji, jeśli chcesz zainstalować zatwierdzone drobne

© Acronis International GmbH, 2003-2024

Opcja	Opis
	aktualizacje.
Aktualizacje określonych produktów (automatyczne zatwierdzanie poprawek i testy)	Użyj tej opcji, jeśli chcesz zdefiniować niestandardowe ustawienia dla różnych produktów. Jeśli chcesz zaktualizować określone produkty, to w przypadku każdego z nich możesz zdefiniować, które aktualizacje mają zostać zainstalowane, na podstawie kategorii, ważności lub statusu zatwierdzenia. Wybierz tę opcję, jeśli chcesz skonfigurować automatyczne zatwierdzanie i testy poprawek.
Instaluj najnowsze wersje tylko w przypadku aplikacji z wykrytymi lukami w zabezpieczeniach	Zaznacz to pole wyboru, jeśli chcesz instalować najnowsze aktualizacje tylko tych aplikacji, w których wykryto luki w zabezpieczeniach*.

* Ta opcja wymaga agenta Cyber Protect w wersji 23.11.36772 lub nowszej.



W przypadku zewnętrznych produktów dla systemu Windows poprawki są dystrybuowane bezpośrednio do obciążeń zarządzanych z wewnętrznej bazy danych Acronis. Jeśli rola Aktualizator jest przypisana do agenta, agent ten będzie używany do pobierania i dystrybuowania poprawek.

Harmonogram

Zdefiniuj harmonogram i warunki, zgodnie z którymi na wybranych komputerach będą instalowane aktualizacje.

© Acronis International GmbH, 2003-2024

Pole	Opis
Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń	To ustawienie umożliwia określenie czasu uruchomienia zadania. Dostępne są następujące wartości: • **Zaplanuj według czasu** — jest to ustawienie domyślne. Zadanie zostanie uruchomione w określonym czasie. • **Gdy użytkownik zaloguje się w systemie** — domyślnie zalogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika. • **Gdy użytkownik wyloguje się z systemu** — domyślnie wylogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika. **Uwaga** Zadanie nie zostanie uruchomione przy zamykaniu systemu. Zamknięcie systemu i wylogowanie to różne zdarzenia w konfiguracji harmonogramu. • **Podczas uruchamiania systemu** — zadanie zostanie uruchomione podczas uruchamiania systemu operacyjnego. • **Podczas zamknięcia systemu** — zadanie zostanie uruchomione podczas zamykania systemu operacyjnego.
Typ harmonogramu	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Dostępne są następujące wartości: • **Co miesiąc** — należy wybrać miesiące i tygodnie lub dni miesiąca, w których zadanie będzie uruchamiane. • **Codziennie** — jest to ustawienie domyślne. Wybierz dni tygodnia, w które będzie uruchamiane zadanie. • **Co godzinę** — należy wybrać dni tygodnia, liczbę powtórzeń oraz przedział czasu, w których zadanie będzie uruchamiane.
Czas rozpoczęcia	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu** Wybierz dokładną godzinę, o której zostanie uruchomione zadanie.
Konfiguruj okno na konserwację na potrzeby poprawek	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Wybierz to ustawienie, jeśli chcesz, aby instalacja poprawek była

© Acronis International GmbH, 2003-2024

Pole	Opis
	uruchamiana tylko w określonym przedziale czasu. Jeśli proces instalacji poprawek nie zostanie ukończony przed upływem czasu określonego przez okno na konserwację na potrzeby poprawek, zostanie on automatycznie zatrzymany.
Uruchom w podanym okresie	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Zaplanuj według czasu**. Ustaw zakres czasu, w którym będzie obowiązywać skonfigurowany harmonogram.
Określ konto użytkownika, którego zalogowanie się w systemie operacyjnym zainicjuje wykonanie zadania	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Gdy użytkownik zaloguje się w systemie**. Dostępne są następujące wartości: • **Dowolny użytkownik** — użyj tej opcji, jeśli chcesz, aby zalogowanie się dowolnego użytkownika powodowało wyzwolenie zadania. • **Następujący użytkownik** — użyj tej opcji, jeśli chcesz, aby tylko zalogowanie się na określonym koncie użytkownika powodowało wyzwolenie zadania.
Określ konto użytkownika, którego wylogowanie się z systemu operacyjnego zainicjuje wykonanie zadania	To pole jest wyświetlane, jeśli w polu **Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń** wybrano opcję **Gdy użytkownik wyloguje się z systemu**. Dostępne są następujące wartości: • **Dowolny użytkownik** — użyj tej opcji, jeśli chcesz, aby wylogowanie się dowolnego użytkownika powodowało wyzwolenie zadania. • **Następujący użytkownik** — użyj tej opcji, jeśli chcesz, aby tylko wylogowanie się z określonego konta użytkownika powodowało wyzwolenie zadania.
Warunki rozpoczęcia	Określ wszystkie warunki, które muszą być jednocześnie spełnione, aby zostało uruchomione zadanie. Warunki rozpoczęcia skanowania pod kątem złośliwego oprogramowania są podobne do warunków uruchomienia modułu **Kopia zapasowa**, które opisano w sekcji „Warunki rozpoczęcia”. Można zdefiniować następujące dodatkowe warunki uruchomienia: • **Rozłóż rozpoczęcie zadania w przedziale czasu** — ta opcja umożliwia zdefiniowanie ram czasowych zadań, aby uniknąć wąskich gardeł na łączach sieciowych. Możesz określić opóźnienie w godzinach lub minutach. Jeśli na przykład domyślną godziną rozpoczęcia jest 10:00, a opóźnienie wynosi 60 minut, to zadanie

© Acronis International GmbH, 2003-2024

Pole	Opis
	rozpocznie się między godziną 10:00 a 11:00. • **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu** • **Zablokuj włączanie trybu uśpienia lub hibernacji podczas wykonywania zadania** — ta opcja działa tylko w przypadku komputerów z systemem Windows. • **Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie po** — określ czas, po którym zadanie zostanie uruchomione, bez względu na spełnienie innych warunków rozpoczęcia. **Uwaga** Warunki uruchomienia nie są obsługiwane w systemie Linux.
Uruchom ponownie po aktualizacji	Określ, czy po ukończeniu instalacji aktualizacji komputer ma być automatycznie uruchamiany ponownie. Dostępne są następujące wartości: • **Nigdy** — po instalacji aktualizacji nigdy nie będzie inicjowane ponowne uruchomienie. • **Jeśli jest to wymagane** — ponowne uruchomienie jest inicjowane tylko wtedy, gdy jest niezbędne do zastosowania aktualizacji. • **Zawsze** — po instalacji aktualizacji zawsze będzie inicjowane ponowne uruchomienie. Można określić opóźnienie ponownego uruchomienia.
Nie uruchamiaj ponownie, dopóki nie zakończy się tworzenie kopii zapasowej	Jeśli zostanie wybrana ta opcja, to w przypadku działania procesu tworzenia kopii zapasowej ponowne uruchomienie komputera zostanie opóźnione do czasu ukończenia operacji tworzenia kopii zapasowej.

Kopia zapasowa przed aktualizacją

Uruchom operację tworzenia kopii zapasowej przed zainstalowaniem aktualizacji oprogramowania — system utworzy przyrostową kopię zapasową komputera, zanim zostanie na nim zainstalowana jakakolwiek aktualizacja. Jeśli jeszcze nie utworzono żadnej kopii zapasowej tego komputera, to zostanie utworzona jego pełna kopia zapasowa. Pozwala to się zabezpieczyć na wypadek niepowodzenia instalacji aktualizacji i konieczności przywrócenia komputera do poprzedniego stanu. Aby opcja **Kopia zapasowa przed aktualizacją** zadziałała, komputery muszą mieć włączone w planie ochrony moduły Zarządzanie poprawkami i Kopia zapasowa oraz odpowiednie elementy do uwzględnienia w kopiach zapasowych — cały komputer lub wolumin rozruchowy i systemowy. W przypadku wybrania niewłaściwych elementów do uwzględnienia w kopii zapasowej, system nie umożliwi włączenia opcji **Kopia zapasowa przed aktualizacją**.

© Acronis International GmbH, 2003-2024

Wyświetlanie listy dostępnych poprawek

Po zakończeniu skanowania w celu oceny luk w zabezpieczeniach informacje o dostępnych poprawkach można znaleźć w sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.

Aby wyświetlić szczegóły dotyczące określonej poprawki, na liście poprawek kliknij odpowiednią poprawkę.

W poniższej tabeli opisano informacje o poprawce widoczne na tym ekranie.

Pole	Opis
Status zatwierdzenia	Status zatwierdzenia jest potrzebny przede wszystkim w przypadku scenariuszy automatycznego zatwierdzania. Możesz zdefiniować jeden z poniższych statusów poprawki: • **Zatwierdzono** — poprawka została zainstalowana na co najmniej jednym komputerze i zatwierdzona jako odpowiednia • **Odmówiono** — poprawka nie jest bezpieczna i może uszkodzić system komputera • **Oczekiwanie na zatwierdzenie** — status poprawki jest niejasny i powinien zostać zweryfikowany
Umowa licencyjna	• Zgadzam się • Odmowa akceptacji. Jeśli nie zgadzasz się na warunki umowy licencyjnej, to poprawka otrzymuje status **Odmówiono** i nie zostaje zainstalowana
Ważność	Poziom ważności poprawki: • **Krytyczne** • **Wysoki** • **Średni** • **Niski** • **Brak**
Dostawca	Dostawca poprawki
Produkt, którego dotyczy problem	Produkt, którego dotyczy poprawka
Zainstalowane wersje	Już zainstalowane wersje produktów
Wersja	Wersja poprawki
Kategoria	Kategoria, do której należy poprawka: • **Aktualizacja krytyczna** — powszechnie udostępniane rozwiązania krytycznych, niezwiązanych z bezpieczeństwem problemów. • **Aktualizacja zabezpieczeń** — powszechnie udostępniane poprawki do

© Acronis International GmbH, 2003-2024

	określonych produktów eliminujące problemy z bezpieczeństwem. • **Aktualizacja definicji** — aktualizacje definicji wirusów lub innych plików definicji. • **Pakiet zbiorczy aktualizacji** — zbiorczy zestaw poprawek, aktualizacji zabezpieczeń, aktualizacji krytycznych i zwykłych aktualizacji zebranych w jednym pakiecie w celu łatwego wdrożenia. Pakiet zbiorczy na ogół jest ukierunkowany na konkretny obszar, np. bezpieczeństwo, lub konkretny komponent, np. usługi Internet Information Services (IIS). • **Dodatek Service Pack** — zbiorczy zestaw wszystkich poprawek, aktualizacji zabezpieczeń, aktualizacji krytycznych i zwykłych aktualizacji utworzonych od czasu wydania produktu. Dodatki Service Pack mogą również zawierać niewielką liczbę zmian projektowych lub funkcjonalnych wprowadzonych na życzenie klientów. • **Narzędzie** — narzędzia lub funkcje, które ułatwiają realizację zadania lub zestawu zadań. • **Pakiet funkcji** — nowe funkcje, zwykle wprowadzane do produktów w nowej wersji. • **Aktualizacja** — powszechnie udostępniane rozwiązania niekrytycznych, niezwiązanych z bezpieczeństwem problemów. • **Aplikacja** — poprawki do aplikacji.
Data wydania	Data wydania poprawki
Ostatni raport	Data ostatniego raportu o poprawce
Pierwsza instalacja	Data pierwszej udanej instalacji poprawki na jakimś komputerze
Microsoft KB	W przypadku poprawki do produktu firmy Microsoft w polu jest podawany identyfikator artykułu z bazy wiedzy
Komputery	Liczba komputerów dotkniętych problemem
Luki w zabezpieczeniach	Liczba luk w zabezpieczeniach. Jej kliknięcie spowoduje przejście do listy luk w zabezpieczeniach.
Rozmiar	Średni rozmiar poprawki
Język	Język obsługiwany przez poprawkę
Witryna dostawcy	Oficjalna witryna internetowa dostawcy poprawki

Konfigurowanie czasu występowania poprawki na liście

Listę poprawek można zaktualizować przez skonfigurowanie na ekranie **Poprawki** czasu występowania danej poprawki na liście. Ustawienie to pozwala określić, jak długo wykryta dostępna poprawka będzie widoczna na liście poprawek. Poprawka zostanie usunięta z listy, gdy zostanie pomyślnie zainstalowana na wszystkich komputerach, na których była oznaczona jako brakująca, lub po upływie okresu ważności na liście.

Aby skonfigurować czas występowania poprawki na liście

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.
2. Kliknij **Ustawienia**.
3. W polu **Czas występowania na liście** wybierz odpowiednią opcję.

Opcja	Opis
Bezterminowo	Poprawka będzie się znajdować na liście przez cały czas.
7 dni	Poprawka zostanie usunięta po siedmiu dniach od jej pierwszej instalacji. Załóżmy na przykład, że masz dwa komputery, na których muszą zostać zainstalowane poprawki. Jeden z nich jest w trybie online, drugi w trybie offline. Poprawka została zainstalowana na pierwszym komputerze. Po 7 dniach poprawka zostanie usunięta z listy poprawek — nawet jeśli nie została zainstalowana na drugim komputerze w związku z tym, że był on w trybie offline.
30 dni	Poprawka zostanie usunięta z listy po 30 dniach od jej pierwszej instalacji.

Automatyczne zatwierdzanie poprawek

Automatyczne zatwierdzanie poprawek ułatwia instalację aktualizacji na komputerach. Dzięki automatycznemu zatwierdzaniu poprawek ich instalacja nie jest opóźniana przez proces ręcznego zatwierdzania poprawek. Owocuje to szybszym instalowaniem ważnych aktualizacji i poprawek, co zwiększa niezawodność systemu.

Automatycznego zatwierdzania poprawek można używać w scenariuszach testowych do automatycznej instalacji poprawek. Jeśli poprawki zostaną pomyślnie zainstalowane na komputerach testowych, zostaną automatycznie zainstalowane na komputerach produkcyjnych. Dodatkowe informacje na temat tego scenariusza można znaleźć w sekcji "Przypadek użycia automatycznego zatwierdzania poprawek i testów" (s. 1054).

Automatycznego zatwierdzania poprawek można też używać do automatycznej instalacji poprawek w środowisku produkcyjnym, z pominięciem fazy testów. Dodatkowe informacje na temat tego scenariusza można znaleźć w sekcji "Przypadek użycia automatycznego zatwierdzania poprawek bez testów" (s. 1057).

Konfigurowanie automatycznego zatwierdzania poprawek

Można skonfigurować automatyczne zatwierdzanie poprawek i w ten sposób zadbać, aby instalacja poprawek nie była opóźniana przez proces ręcznego zatwierdzania poprawek.

Aby skonfigurować automatyczne zatwierdzanie poprawek

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.
2. Kliknij **Ustawienia**.
3. Włącz **Automatyczne zatwierdzanie poprawek**.

© Acronis International GmbH, 2003-2024

4. Skonfiguruj ustawienia na potrzeby automatycznego zatwierdzania poprawek.
   a. Wybierz opcję automatycznego zatwierdzania poprawek.

Opcja	Opis
Automatyczne zatwierdzanie poprawek i testy	Po upływie wybranej liczby dni od pomyślnego zainstalowania poprawki status zatwierdzenia poprawki zmieni się na **Zatwierdzono**. Ustawienia tego warto użyć, jeśli chcesz przetestować poprawki przez zainstalowanie ich najpierw na komputerze testowym, aby się upewnić, że wszystko działa zgodnie z oczekiwaniami, a dopiero potem zainstalować poprawki w środowisku produkcyjnym.
Automatyczne zatwierdzanie poprawek bez testów	Po upływie wybranej liczby dni od znalezienia poprawki status zatwierdzenia poprawki zmieni się na **Zatwierdzono**.

   b. Wybierz liczbę dni, które muszą upłynąć od spełnienia warunku opcji automatycznego zatwierdzania poprawek. Po tym okresie status zatwierdzenia poprawek zostanie automatycznie zmieniony z **Oczekiwanie na zatwierdzenie** na **Zatwierdzono**.
5. Wybierz **Automatycznie zaakceptuj umowy licencyjne**.
6. Kliknij **Zastosuj**.

Przypadek użycia automatycznego zatwierdzania poprawek i testów

Jeśli chcesz przetestować nowe poprawki na komputerze testowym, zanim zostaną zainstalowane na komputerach produkcyjnych, możesz skonfigurować dwa plany ochrony: plan instalacji poprawek do celów testowych i plan instalacji przetestowanych poprawek na komputerach produkcyjnych. Dzięki temu upewnisz się, że poprawki instalowane w środowisku produkcyjnym są bezpieczne i komputery produkcyjne będą działać poprawnie po zainstalowaniu tych poprawek.

Procedura składa się z następujących etapów:

1. Skonfiguruj ustawienia na potrzeby automatycznego zatwierdzania poprawek. Wybierz opcję **Automatyczne zatwierdzanie poprawek i testy**. Aby uzyskać więcej informacji, zobacz "Konfigurowanie automatycznego zatwierdzania poprawek" (s. 1053).
2. Skonfiguruj plan ochrony na potrzeby testu (na przykład „Poprawki testowe”) z włączonym modułem **Zarządzanie poprawkami** i zastosuj go do komputerów w środowisku testowym. Określ następujący warunek instalacji poprawek: status zatwierdzenia poprawki musi mieć wartość **Oczekiwanie na zatwierdzenie**. Ten krok jest potrzebny do weryfikacji poprawek i sprawdzenia, czy komputery działają prawidłowo po ich zainstalowaniu. Aby uzyskać więcej informacji, zobacz "Konfigurowanie planu ochrony Poprawki testowe" (s. 1055).
3. Skonfiguruj plan ochrony na potrzeby środowiska produkcyjnego (na przykład „Poprawki produkcyjne”) z włączonym modułem **Zarządzanie poprawkami** i zastosuj go do komputerów w środowisku produkcyjnym. Określ następujący warunek instalacji poprawek: status poprawki

© Acronis International GmbH, 2003-2024

musi mieć wartość **Zatwierdzono**. Aby uzyskać więcej informacji, zobacz "Konfigurowanie planu ochrony Poprawki produkcyjne" (s. 1056).

4. Uruchom plan Poprawki testowe i sprawdź wyniki. Zostaw status zatwierdzenia komputerów, w których przypadku nie występują problemy, jako **Oczekiwanie na zatwierdzenie**, ale zmień status zatwierdzenia niepoprawnie działających komputerów na **Odmówiono**. Na podstawie liczby dni określonej w ustawieniu **Automatyczne zatwierdzanie poprawek** status poprawek zostanie automatycznie zmieniony z **Oczekiwanie na zatwierdzenie** na **Zatwierdzono**. W wyniku uruchomienia planu Poprawki produkcyjne na komputerach produkcyjnych zostaną uruchomione tylko poprawki ze statusem **Zatwierdzono**. Aby uzyskać więcej informacji, zobacz "Uruchamianie planu ochrony Poprawki testowe i odrzucanie niebezpiecznych poprawek" (s. 1057).
5. Uruchom plan Poprawki produkcyjne.

Konfigurowanie planu ochrony Poprawki testowe

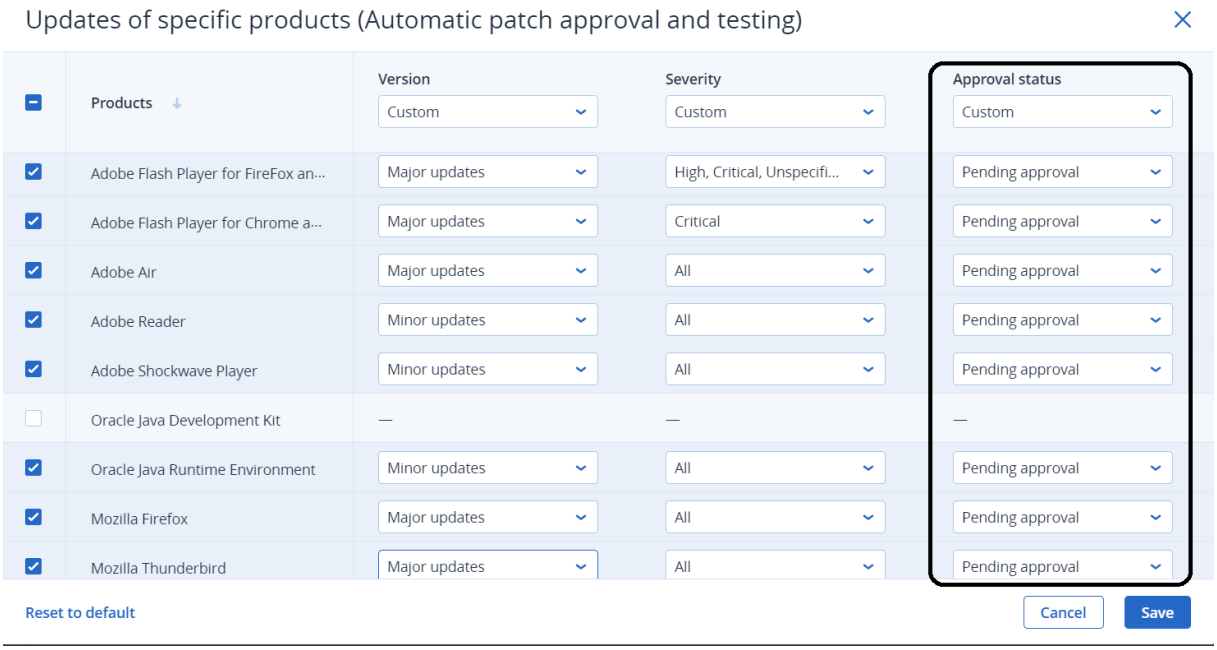
Istnieje możliwość skonfigurowania planu ochrony z ustawieniami instalacji poprawek dla komputerów działających w środowisku testowym.

Aby skonfigurować plan ochrony Poprawki testowe

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Kliknij **Utwórz plan**.
3. Włącz moduł **Zarządzanie poprawkami**.
4. Określ, które aktualizacje produktów firmy Microsoft i innych firm mają zostać zainstalowane, zaplanuj tę operację w harmonogramie i utwórz kopię zapasową przed aktualizacją. Dodatkowe informacje na temat tych ustawień można znaleźć w sekcji "Ustawienia zarządzania poprawkami w planie ochrony" (s. 1045).

Ważne
W przypadku wszystkich aktualizowanych produktów należy określić status zatwierdzenia **Oczekiwanie na zatwierdzenie**. Dzięki temu agent zainstaluje tylko poprawki ze statusem **Oczekiwanie na zatwierdzenie** na wybranych komputerach w środowisku testowym.

© Acronis International GmbH, 2003-2024



Konfigurowanie planu ochrony Poprawki produkcyjne

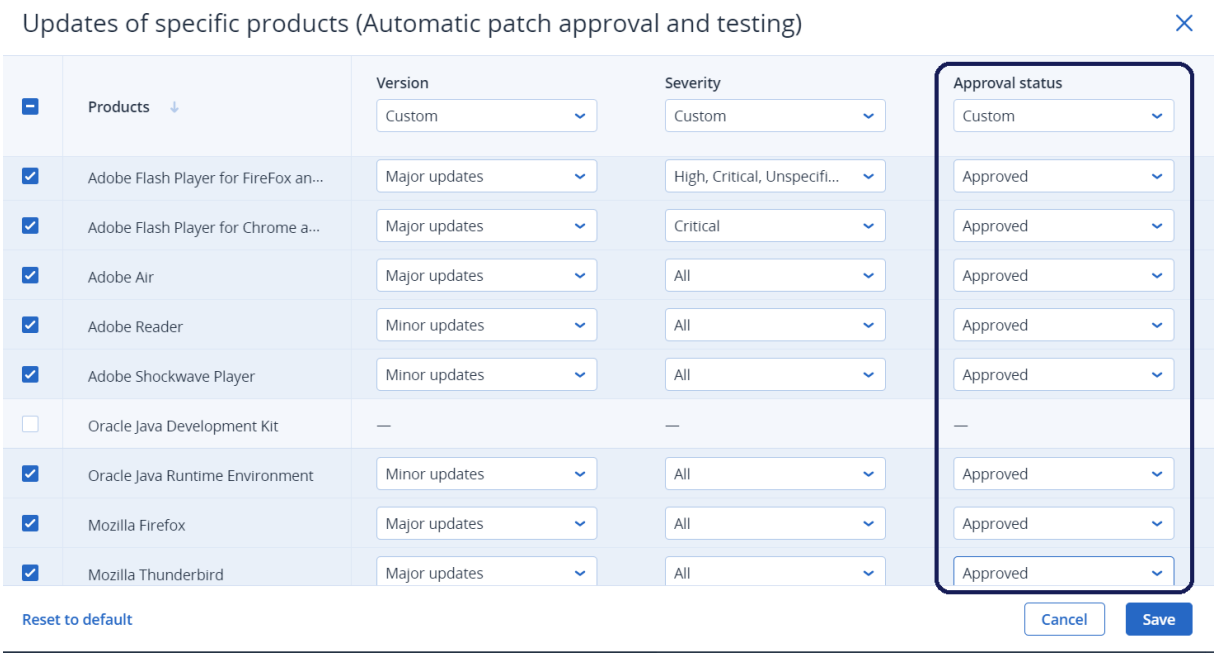
Istnieje możliwość skonfigurowania planu ochrony z ustawieniami instalacji poprawek dla komputerów działających w środowisku produkcyjnym.

Aby skonfigurować plan ochrony Poprawki produkcyjne

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany ochrony**.
2. Kliknij **Utwórz plan**.
3. Włącz moduł **Zarządzanie poprawkami**.
4. Określ, które aktualizacje produktów firmy Microsoft i innych firm mają zostać zainstalowane, zaplanuj tę operację w harmonogramie i utwórz kopię zapasową przed aktualizacją. Dodatkowe informacje na temat tych ustawień można znaleźć w sekcji "Ustawienia zarządzania poprawkami w planie ochrony" (s. 1045).

Ważne
W przypadku wszystkich aktualizowanych produktów ustaw **Status zatwierdzenia** jako **Zatwierdzono**. Dzięki temu agent zainstaluje na wybranych komputerach w środowisku produkcyjnym tylko poprawki ze statusem **Zatwierdzono**.

© Acronis International GmbH, 2003-2024



Uruchamianie planu ochrony Poprawki testowe i odrzucanie niebezpiecznych poprawek

Po zainstalowaniu poprawek na komputerach w środowisku testowym można sprawdzić, czy wszystko działa zgodnie z oczekiwaniami. Możesz zostawić status zatwierdzenia komputerów, w których przypadku nie występują problemy, jako **Oczekiwanie na zatwierdzenie**, a zmienić status zatwierdzenia niepoprawnie działających komputerów na **Odmówiono**.

Aby uruchomić plan ochrony Poprawki testowe i odrzucić niebezpieczne poprawki

1. Uruchom plan ochrony Poprawki testowe (według harmonogramu lub ręcznie).
2. Na podstawie uzyskanych wyników sprawdź, które z zainstalowanych poprawek są bezpieczne.
3. Przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki** i w przypadku poprawek, które nie są bezpieczne, ustaw **Status zatwierdzenia** jako **Odmówiono**.

Przypadek użycia automatycznego zatwierdzania poprawek bez testów

Jeśli chcesz, aby nowe poprawki były jak najszybciej automatycznie instalowane na komputerach produkcyjnych bez uprzedniego instalowania ich na komputerach testowych, możesz skonfigurować tylko jeden plan ochrony.

Procedura składa się z następujących etapów:

1. Skonfiguruj ustawienia na potrzeby automatycznego zatwierdzania poprawek. Wybierz opcję **Automatyczne zatwierdzanie poprawek bez testów**. Aby uzyskać więcej informacji, zobacz "Konfigurowanie automatycznego zatwierdzania poprawek" (s. 1053).
2. Skonfiguruj plan ochrony na potrzeby środowiska produkcyjnego (na przykład „Poprawki produkcyjne”) z włączonym modułem **Zarządzanie poprawkami** i zastosuj go do komputerów w środowisku produkcyjnym. Określ następujący warunek instalacji poprawek: status poprawki

© Acronis International GmbH, 2003-2024

musi mieć wartość **Zatwierdzono**. Aby uzyskać więcej informacji, zobacz "Konfigurowanie planu ochrony Poprawki produkcyjne" (s. 1056).

3. Uruchom plan Poprawki produkcyjne.

Ręczne zatwierdzanie poprawek

Możesz ręcznie zatwierdzić poprawkę i przyspieszyć jej instalację, pomijając fazę testowania.

Wymagania wstępne

- Plan ochrony z włączonym modułem **Zarządzanie poprawkami** zastosowano do co najmniej jednego komputera z systemem Windows.
- Istnieją poprawki, które nadal nie zostały zainstalowane na komputerach, na których zastosowano plan ochrony.

Aby ręcznie zatwierdzić poprawki

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.
2. Wybierz poprawki, które chcesz zainstalować, a następnie zaakceptuj ich umowy licencyjne.
3. Ustaw **Status zatwierdzenia** poprawek na **Zatwierdzono**.
   Status zatwierdzenia poprawek jest ustawiony na **Zatwierdzono**. Poprawki będą automatycznie instalowane na komputerach zgodnie z harmonogramem zdefiniowanym w planie ochrony. Jeśli chcesz zainstalować poprawki od razu, wykonaj procedurę opisaną w sekcji "Instalowanie poprawek na żądanie" (s. 1058).

Instalowanie poprawek na żądanie

Jeśli nie chcesz czekać na zaplanowany czas instalacji, możesz zainstalować poprawki ręcznie na żądanie.

Ręczną instalację poprawek można zainicjować na trzech ekranach: **Poprawki**, **Luki w zabezpieczeniach** i **Wszystkie urządzenia**.

Aby ręcznie zainstalować poprawkę

Na ekranie Poprawki

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.
2. Zaakceptuj umowy licencyjne poprawek, które chcesz zainstalować.
3. W kreatorze **Zainstaluj poprawki** wybierz poprawki, które chcesz zainstalować, a następnie kliknij **Zainstaluj**.
4. Wybierz komputery, na których chcesz zainstalować poprawki.
5. Wybierz opcje ponownego uruchomienia.

© Acronis International GmbH, 2003-2024

a. Wybierz, czy komputer ma zostać uruchomiony ponownie po zainstalowaniu poprawek.

Opcja	Opis
Nie	Komputery nie zostaną automatycznie uruchomione ponownie po zainstalowaniu poprawek.
Jeśli jest to wymagane	Komputery zostaną uruchomione ponownie tylko wtedy, gdy jest to niezbędne do zastosowania poprawek.
Tak	Komputery zostaną automatycznie uruchomione ponownie po zainstalowaniu poprawek. Można też określić opóźnienie ponownego uruchomienia.

b. [Opcjonalnie] Jeśli chcesz opóźnić ponowne uruchomienie komputera o czas tworzenia jego kopii zapasowej, wybierz **Nie uruchamiaj ponownie, dopóki nie zakończy się tworzenie kopii zapasowej**.

6. Kliknij **Zainstaluj poprawki**.

Na ekranie Luki w zabezpieczeniach

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Luki w zabezpieczeniach**.
2. Przeprowadź proces naprawczy zgodnie z opisem podanym w sekcji "Zarządzanie znalezionymi lukami w zabezpieczeniach" (s. 1042).

W sekcji Wszystkie urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputer, na którym chcesz zainstalować poprawki.
3. Kliknij **Poprawka**.
4. Wybierz poprawki, które chcesz zainstalować, i kliknij **Dalej**.
5. Wybierz opcje ponownego uruchomienia.
   a. Wybierz, czy komputer ma zostać uruchomiony ponownie po zainstalowaniu poprawek.

Opcja	Opis
Nie	Komputery nie zostaną automatycznie uruchomione ponownie po zainstalowaniu poprawek.
Jeśli jest to wymagane	Komputery zostaną uruchomione ponownie tylko wtedy, gdy jest to niezbędne do zastosowania poprawek.
Tak	Komputery zostaną automatycznie uruchomione ponownie po zainstalowaniu poprawek. Można też określić opóźnienie ponownego uruchomienia.

   b. [Opcjonalnie] Jeśli chcesz opóźnić ponowne uruchomienie komputera o czas tworzenia jego

© Acronis International GmbH, 2003-2024

kopii zapasowej, wybierz **Nie uruchamiaj ponownie, dopóki nie zakończy się tworzenie kopii zapasowej**.

6. Kliknij **Zainstaluj poprawki**.

© Acronis International GmbH, 2003-2024

Zarządzanie inwentaryzacją oprogramowania i sprzętu

Inwentaryzacja oprogramowania

Funkcja inwentaryzacji oprogramowania jest dostępna w przypadku tych urządzeń, na których jest włączony pakiet Advanced lub które mają starszą licencję programu Cyber Protect (Legacy). Funkcja ta umożliwia przeglądanie wszystkich aplikacji dostępnych na wszystkich urządzeniach z systemem Windows i macOS.

Aby uzyskać dane inwentaryzacyjne dotyczące oprogramowania, można uruchomić automatyczne lub ręczne skanowanie urządzeń.

Dane inwentaryzacyjne dotyczące oprogramowania umożliwiają:

- przeglądanie i porównywanie informacji o wszystkich aplikacjach zainstalowanych na urządzeniach firmy;
- ustalanie ewentualnej konieczności zaktualizowania aplikacji;
- ustalanie ewentualnej konieczności usunięcia nieużywanej aplikacji;
- sprawdzanie, czy wersja oprogramowania na wielu urządzeniach firmy jest taka sama;
- monitorowanie zmian statusów oprogramowania między kolejnymi operacjami skanowania.

Włączanie skanowania w celu inwentaryzacji oprogramowania

W przypadku włączenia na urządzeniach skanowania w celu inwentaryzacji oprogramowania system automatycznie zbiera dane o oprogramowaniu co 12 godzin.

Funkcja Skanowanie w celu inwentaryzacji oprogramowania jest domyślnie włączona w przypadku wszystkich urządzeń, które mają wymaganą licencję, ale w razie potrzeby można to ustawienie zmienić.

Uwaga
Dzierżawcy-klienci mogą włączać lub wyłączać skanowanie w celu inwentaryzacji oprogramowania. Dzierżawcy-jednostki mogą tylko wyświetlać ustawienia skanowania w celu inwentaryzacji oprogramowania, ale nie mogą ich zmieniać.

Aby włączyć skanowanie w celu inwentaryzacji oprogramowania

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia**.
2. Kliknij **Ochrona**.
3. Kliknij **Skanowanie inwentaryzacyjne**.
4. Włącz moduł **Skanowanie w celu inwentaryzacji oprogramowania**, klikając przełącznik obok jego nazwy.

© Acronis International GmbH, 2003-2024

Aby wyłączyć skanowanie w celu inwentaryzacji oprogramowania

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia**.
2. Kliknij **Ochrona**.
3. Kliknij **Skanowanie inwentaryzacyjne**.
4. Wyłącz moduł **Skanowanie w celu inwentaryzacji oprogramowania**, klikając przełącznik obok jego nazwy.

Ręczne uruchamianie skanowania w celu inwentaryzacji oprogramowania

Skanowanie w celu inwentaryzacji oprogramowania można uruchomić ręcznie na ekranie **Inwentaryzacja oprogramowania** lub na karcie **Oprogramowanie** na ekranie **Inwentaryzacja**.

Wymagania wstępne

- Urządzenie ma zainstalowany system operacyjny Windows lub macOS.
- Urządzenie ma wymaganą starszą licencję programu Cyber Protect (Legacy) lub aktywowany pakiet Zarządzanie zaawansowane.

Aby uruchomić skanowanie w celu inwentaryzacji oprogramowania na ekranie Inwentaryzacja oprogramowania

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem**.
2. Kliknij **Inwentaryzacja oprogramowania**.
3. W polu rozwijanym **Grupuj według** wybierz **Urządzenia**.
4. Znajdź urządzenie, które chcesz przeskanować, i kliknij **Skanuj**.

Aby uruchomić skanowanie w celu inwentaryzacji oprogramowania na karcie Oprogramowanie na ekranie Inwentaryzacja

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Kliknij urządzenie, które chcesz przeskanować, a następnie kliknij **Inwentaryzacja**.
3. Na karcie **Oprogramowanie** kliknij **Skanuj**.

Przeglądanie wyników inwentaryzacji oprogramowania

Można przeglądać i analizować dane dotyczące wszystkich aplikacji dostępnych na wszystkich urządzeniach firmy.

© Acronis International GmbH, 2003-2024

Wymagania wstępne

- Urządzenia mają zainstalowany system operacyjny Windows lub macOS.
- Urządzenia mają wymaganą starszą licencję programu Cyber Protect (Legacy) lub aktywowany pakiet Zarządzanie zaawansowane.
- Skanowanie urządzeń w celu inwentaryzacji oprogramowania zakończyło się pomyślnie.

Aby wyświetlić wszystkie aplikacje dostępne na wszystkich urządzeniach firmy z systemem Windows i macOS

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem**.
2. Kliknij **Inwentaryzacja oprogramowania**.
   Domyślnie dane są pogrupowane według urządzeń. W poniższej tabeli przedstawiono dane widoczne na ekranie **Inwentaryzacja oprogramowania**.

Kolumna	Opis
Nazwa	Nazwa aplikacji.
Wersja	Wersja aplikacji.
Status	Status aplikacji. • **Nowa**. • **Zaktualizowano**. • **Usunięto**. • **Brak zmian**.
Dostawca	Dostawca aplikacji.
Data instalacji	Data i godzina zainstalowania aplikacji.
Ostatni przebieg	Tylko w przypadku urządzeń z systemem macOS. Data i godzina ostatniej aktywności aplikacji.
Lokalizacja	Katalog, w którym została zainstalowana aplikacja.
Użytkownik	Użytkownik, który zainstalował aplikację.
Typ systemu	Tylko w przypadku urządzeń z systemem Windows. Bitowość aplikacji. • **X86** w przypadku aplikacji 32-bitowych. • **X64** w przypadku aplikacji 64-bitowych.

3. Aby pogrupować dane według aplikacji, w polu rozwijanym **Grupuj według** wybierz **Aplikacje**.
4. Aby zawęzić informacje wyświetlane na ekranie, użyj co najmniej jednego filtru.
   a. Kliknij **Filtruj**.
   b. Wybierz co najmniej jeden filtr.

© Acronis International GmbH, 2003-2024

W poniższej tabeli przedstawiono filtry widoczne na ekranie **Inwentaryzacja oprogramowania**.

Filtr	Opis
Nazwa urządzenia	Nazwa urządzenia. Można wybrać kilka opcji. Za pomocą tego filtru można porównać oprogramowanie dostępne na wybranych urządzeniach.
Aplikacja	Nazwa aplikacji. Można wybrać kilka opcji. Za pomocą tego filtru można porównać dane dotyczące określonej aplikacji dostępnej na wybranych lub wszystkich urządzeniach.
Dostawca	Dostawca aplikacji. Można wybrać kilka opcji. Za pomocą tego filtru można wyświetlić wszystkie aplikacje określonego dostawcy dostępne na wybranych lub wszystkich urządzeniach.
Status	Status aplikacji. Można wybrać kilka opcji. Za pomocą tego filtru można wyświetlić wszystkie aplikacje o wskazanym statusie dostępne na wybranych lub wszystkich urządzeniach.
Data instalacji	Dzień instalacji aplikacji. Za pomocą tego filtru można wyświetlić wszystkie aplikacje zainstalowane we wskazanym dniu na wybranych lub wszystkich urządzeniach.
Data skanowania	Data skanowania w celu inwentaryzacji oprogramowania. Za pomocą tego filtru można wyświetlić informacje o oprogramowaniu na wybranych lub wszystkich urządzeniach przeskanowanym we wskazanym dniu.

c. Kliknij **Zastosuj**.

5. Aby przejrzeć całą listę z inwentaryzacji oprogramowania, skorzystaj z opcji paginacji w lewej dolnej części ekranu.

- Kliknij numer strony, którą chcesz otworzyć.
- W polu rozwijanym kliknij numer strony, którą chcesz otworzyć.

Wyświetlanie wyników inwentaryzacji oprogramowania wybranego urządzenia

Można wyświetlić listę wszystkich aplikacji zainstalowanych na wybranym urządzeniu, a także szczegółowe informacje o tych aplikacjach, takie jak status, wersja, dostawca, data instalacji, ostatnie uruchomienie i lokalizacja.

© Acronis International GmbH, 2003-2024

Wymagania wstępne

- Urządzenie ma zainstalowany system operacyjny Windows lub macOS.
- Urządzenie ma wymaganą starszą licencję programu Cyber Protect (Legacy) lub aktywowany pakiet Zarządzanie zaawansowane.
- Skanowanie urządzenia w celu inwentaryzacji oprogramowania zakończyło się pomyślnie.

Aby wyświetlić wyniki inwentaryzacji oprogramowania wybranego urządzenia z poziomu ekranu Inwentaryzacja oprogramowania

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem**.
2. Kliknij **Inwentaryzacja oprogramowania**.
3. W polu rozwijanym **Grupuj według** wybierz **Urządzenia**.
4. Znajdź urządzenie, które chcesz sprawdzić, korzystając z jednej z poniższych opcji.
   - Znajdź urządzenie przy użyciu opcji **Filtruj**:
     a. Kliknij **Filtruj**.
     b. W polu **Nazwa urządzenia** wybierz nazwę urządzenia, które chcesz wyświetlić.
     c. Kliknij **Zastosuj**.
   - Znajdź urządzenie przy użyciu działającej dynamicznie opcji **Wyszukaj**:
     a. Kliknij **Wyszukaj**.
     b. Wpisz całą nazwę urządzenia lub jej część.

Aby wyświetlić wyniki inwentaryzacji oprogramowania wybranego urządzenia z poziomu ekranu Urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Kliknij urządzenie, które chcesz wyświetlić, a następnie kliknij **Inwentaryzacja**.
3. Kliknij kartę **Oprogramowanie**.

Inwentaryzacja sprzętu

Funkcja inwentaryzacji sprzętu umożliwia przeglądanie wszystkich elementów sprzętowych dostępnych w:

- urządzeniach fizycznych z systemem Windows i macOS i licencją obsługującą funkcję Inwentaryzacja sprzętu;
- maszynach wirtualnych z systemem Windows i macOS działających na następujących platformach wirtualizacji: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo i Virtuozzo Hybrid Infrastructure. Więcej informacji o obsługiwanych wersjach platform wirtualizacji można znaleźć w sekcji "Obsługiwane platformy wirtualizacji" (s. 32).

© Acronis International GmbH, 2003-2024

Uwaga
Funkcja Inwentaryzacja sprzętu w odniesieniu do maszyn wirtualnych nie jest obsługiwana w starszych wersjach programu Cyber Protect.

Funkcja Inwentaryzacja sprzętu jest obsługiwana tylko w przypadku urządzeń, na których jest zainstalowany agent ochrony.

Aby uzyskać dane inwentaryzacyjne dotyczące sprzętu, można uruchomić automatyczne lub ręczne skanowanie urządzeń.

Dane inwentaryzacyjne dotyczące sprzętu umożliwiają:

- wykrywanie wszystkich zasobów sprzętowych organizacji,
- przeglądanie zasobów sprzętowych wszystkich urządzeń organizacji,
- porównywanie elementów sprzętowych wielu urządzeń firmy,
- wyświetlanie szczegółowych informacji o danym elemencie sprzętowym.

Włączanie skanowania w celu inwentaryzacji sprzętu

W przypadku włączenia skanowania w celu inwentaryzacji sprzętu na urządzeniach fizycznych i maszynach wirtualnych system automatycznie zbiera dane o sprzęcie co 12 godzin.

Funkcja skanowania w celu inwentaryzacji sprzętu jest domyślnie włączona, ale w razie potrzeby można to ustawienie zmienić.

Uwaga
Dzierżawcy-klienci mogą włączać lub wyłączać skanowanie w celu inwentaryzacji sprzętu. Dzierżawcy-jednostki mogą tylko wyświetlać ustawienia skanowania w celu inwentaryzacji sprzętu, ale nie mogą ich zmieniać.

Aby włączyć skanowanie w celu inwentaryzacji sprzętu

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia**.
2. Kliknij **Ochrona**.
3. Kliknij **Skanowanie inwentaryzacyjne**.
4. Włącz moduł **Skanowanie w celu inwentaryzacji sprzętu**, klikając przełącznik obok jego nazwy.

Aby wyłączyć skanowanie w celu inwentaryzacji sprzętu

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia**.
2. Kliknij **Ochrona**.
3. Kliknij **Skanowanie inwentaryzacyjne**.
4. Wyłącz moduł **Skanowanie w celu inwentaryzacji sprzętu**, klikając przełącznik obok jego nazwy.

© Acronis International GmbH, 2003-2024

Ręczne uruchamianie skanowania w celu inwentaryzacji sprzętu

Istnieje możliwość ręcznego uruchomienia skanowania w celu inwentaryzacji sprzętu wybranego urządzenia i przejrzenia bieżących danych dotyczących elementów sprzętowych tego urządzenia.

Uwaga
Skanowanie w celu inwentaryzacji sprzętu maszyn wirtualnych jest obsługiwane tylko wtedy, gdy bieżąca data i godzina maszyny wirtualnej odpowiada bieżącej dacie i godzinie według strefy UTC. Aby maszyna wirtualna na pewno używała prawidłowych ustawień czasu, wyłącz opcję **Synchronizacja czasu** maszyny wirtualnej, ustaw bieżącą datę, godzinę i strefę czasową, a następnie uruchom ponownie usługi **Acronis Agent Core Service** i **Acronis Managed Machine Service**.

Wymagania wstępne

- (W przypadku wszystkich urządzeń) Urządzenie korzysta z systemu operacyjnego Windows lub macOS.
- (Dotyczy wszystkich urządzeń) Urządzenia mają licencję obsługującą funkcję Inwentaryzacja sprzętu. Uwaga: funkcja Inwentaryzacja sprzętu w odniesieniu do maszyn wirtualnych nie jest obsługiwana w starszych wersjach programu Cyber Protect (Legacy).
- (W przypadku wszystkich urządzeń) Na urządzeniu jest zainstalowany agent ochrony.
- (W przypadku maszyn wirtualnych) Maszyna działa na jednej z obsługiwanych platform wirtualizacji. Aby uzyskać więcej informacji, zobacz "Inwentaryzacja sprzętu" (s. 1065).

Aby uruchomić skanowanie w celu inwentaryzacji sprzętu jednego urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Kliknij urządzenie, które chcesz przeskanować, a następnie kliknij **Inwentaryzacja**.
3. Na karcie **Sprzęt** kliknij **Skanuj**.

Przeglądanie wyników inwentaryzacji sprzętu

Można przeglądać i analizować dane dotyczące wszystkich elementów sprzętowych dostępnych we wszystkich urządzeniach firmy.

Wymagania wstępne

- (W przypadku wszystkich urządzeń) Urządzenia mają zainstalowany system operacyjny Windows lub macOS.
- (W przypadku wszystkich urządzeń) Urządzenia mają licencję obsługującą funkcję Inwentaryzacja sprzętu. Uwaga: funkcja Inwentaryzacja sprzętu w odniesieniu do maszyn wirtualnych nie jest obsługiwana w starszych wersjach programu Cyber Protect.
- (W przypadku wszystkich urządzeń) Na urządzeniu jest zainstalowany agent ochrony.

© Acronis International GmbH, 2003-2024

- (W przypadku wszystkich urządzeń) Skanowanie urządzeń w celu inwentaryzacji sprzętu zakończyło się pomyślnie.
- (W przypadku maszyn wirtualnych) Maszyna działa na jednej z obsługiwanych platform wirtualizacji. Aby uzyskać więcej informacji, zobacz "Inwentaryzacja sprzętu" (s. 1065).

Aby wyświetlić wszystkie elementy sprzętowe dostępne w urządzeniach firmy z systemem Windows i macOS

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. W polu rozwijanym **Widok** wybierz **Sprzęt**.

Uwaga
Widok obejmuje zestaw kolumn, które określają, jakie dane są widoczne na ekranie. W oprogramowaniu są gotowe widoki **Standardowy** i **Sprzęt**. Można tworzyć oraz zapisywać niestandardowe widoki obejmujące różne, lepiej przystosowane do określonych potrzeb zestawy kolumn.

W poniższej tabeli przedstawiono dane widoczne w widoku **Sprzęt**.

Kolumna	Opis
Nazwa	Nazwa urządzenia.
Status skanowania sprzętu	Status operacji skanowania dotyczącego sprzętu. • **Ukończono**. • **Nie uruchomiono**. • **Nieobsługiwane** — status pokazywany w przypadku obciążeń, w których przypadku nie jest obsługiwana funkcja inwentaryzacji sprzętu, tj. maszyn wirtualnych, urządzeń mobilnych, urządzeń z systemem Linux. • **Aktualizuj agenta**. Status pokazywany w przypadku, gdy na urządzeniu jest zainstalowana nieaktualna wersja agenta. Kliknięcie tej pozycji spowoduje przekierowanie do strony Ustawienia > Agenci, na której administrator może zaktualizować agenta. • **Zwiększ limit**. Kliknięcie tej pozycji spowoduje otwarcie okna dialogowego, w którym administrator może zamienić bieżącą licencję na jedną z innych dostępnych licencji dzierżawcy.
Procesor	Modele wszystkich procesorów urządzenia.
Rdzenie procesora	Liczba rdzeni wszystkich procesorów urządzenia.
Miejsce na dysku	Wykorzystane miejsce oraz całkowita ilość miejsca

© Acronis International GmbH, 2003-2024

Kolumna	Opis
	na wszystkich dyskach urządzenia.
Pamięć	Łączna pojemność pamięci RAM urządzenia.
Data skanowania	Data i godzina ostatniego skanowania w celu inwentaryzacji sprzętu.
Płyta główna	Płyta główna urządzenia.
Numer seryjny płyty głównej	Numer seryjny płyty głównej.
Wersja systemu BIOS	Wersja systemu BIOS.
Organizacja	Organizacja, do której należy urządzenie.
Właściciel	Właściciel urządzenia.
Domena	Domena urządzenia.
System operacyjny	System operacyjny urządzenia.
Kompilacja systemu operacyjnego	Kompilacja systemu operacyjnego urządzenia.

3. Aby dodać kolumny do tabeli, kliknij ikonę opcji kolumn i wybierz kolumny, które mają być widoczne w tabeli.
4. Aby zawęzić informacje wyświetlane na ekranie, użyj co najmniej jednego filtru.
   a. Kliknij **Wyszukaj**.
   b. Kliknij strzałkę, a następnie kliknij **Sprzęt**.
   c. Wybierz co najmniej jeden filtr.
      W poniższej tabeli przedstawiono filtry widoku **Sprzęt**.

Filtr	Opis
Model procesora	Można wybrać kilka opcji. Za pomocą tego filtru można wyświetlić dane dotyczące sprzętu w urządzeniach z określonym modelem procesora.
Rdzenie procesora	Za pomocą tego filtru można wyświetlić dane dotyczące sprzętu w urządzeniach z określoną liczbą rdzeni procesora.
Łączny rozmiar dysków	Za pomocą tego filtru można wyświetlić dane dotyczące sprzętu w urządzeniach z określoną pojemnością pamięci masowej.
Pojemność pamięci	Za pomocą tego filtru można wyświetlić dane dotyczące sprzętu w urządzeniach z określoną pojemnością pamięci RAM.

   d. Kliknij **Zastosuj**.
5. Aby posortować dane w kolejności rosnącej, należy kliknąć nazwę kolumny.

© Acronis International GmbH, 2003-2024

Wyświetlanie sprzętu wybranego urządzenia

Dostępna jest możliwość wyświetlenia szczegółowych informacji o płycie głównej, procesorach, pamięci, karcie graficznej, pamięci masowej, sieci i systemie określonego urządzenia.

Wymagania wstępne

- (W przypadku wszystkich urządzeń) Urządzenie korzysta z systemu operacyjnego Windows lub macOS.
- (W przypadku wszystkich urządzeń) Urządzenia mają licencję obsługującą funkcję Inwentaryzacja sprzętu. Uwaga: funkcja Inwentaryzacja sprzętu w odniesieniu do maszyn wirtualnych nie jest obsługiwana w starszych wersjach programu Cyber Protect.
- (W przypadku wszystkich urządzeń) Na urządzeniu jest zainstalowany agent ochrony.
- (W przypadku wszystkich urządzeń) Skanowanie urządzenia w celu inwentaryzacji sprzętu zakończyło się pomyślnie.
- (W przypadku maszyn wirtualnych) Maszyna działa na jednej z obsługiwanych platform wirtualizacji. Aby uzyskać więcej informacji, zobacz "Inwentaryzacja sprzętu" (s. 1065).

Aby wyświetlić szczegółowe informacje na temat sprzętu wybranego urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. W polu rozwijanym **Widok** wybierz **Sprzęt**.
3. Znajdź urządzenie, które chcesz sprawdzić, korzystając z jednej z metod opisanych poniżej.
   - Znajdź urządzenie przy użyciu opcji **Filtruj**:
     a. Kliknij **Filtruj**.
     b. Wybierz parametry filtru, aby znaleźć urządzenie.
     c. Kliknij **Zastosuj**.
   - Znajdź urządzenie przy użyciu opcji **Wyszukaj**:
     a. Kliknij **Wyszukaj**.
     b. Wpisz całą nazwę urządzenia lub jej część, a następnie naciśnij klawisz **Enter**.
4. Wybierz wiersz z urządzeniem i kliknij **Inwentaryzacja**.
5. Kliknij kartę **Sprzęt**.

   Dostępne są następujące dane na temat sprzętu.

Element sprzętowy	Wyświetlane informacje
Płyta główna	Nazwa, producent, model i numer seryjny płyty głównej urządzenia.
Procesory	Producent, model, maksymalna szybkość zegara i liczba rdzeni poszczególnych procesorów urządzenia.

© Acronis International GmbH, 2003-2024

Element sprzętowy	Wyświetlane informacje
Pamięć	Pojemność, producent i numer seryjny pamięci operacyjnej urządzenia.
Karta graficzna	Producent i model procesora graficznego urządzenia.
Dyski magazynowania	Model, typ nośnika, dostępne miejsce i pojemność dysków urządzenia.
Sieć	Adres MAC, adres IP oraz typ kart sieciowych urządzenia.
System	Identyfikator produktu, data pierwszej instalacji, czas rozruchu systemu, producent systemu, model systemu, wersja systemu BIOS, urządzenie rozruchowe, ustawienia regionalne systemu i strefa czasowa systemu.

© Acronis International GmbH, 2003-2024

Nawiązywanie połączeń z zarządzanymi obciążeniami na potrzeby pulpitu zdalnego lub pomocy zdalnej

Funkcja pulpitu zdalnego i pomocy zdalnej to wygodny sposób na nawiązywanie połączenia z obciążeniami w organizacji na potrzeby zdalnego sterowania lub pomocy zdalnej. Od grudnia 2022 roku funkcja ta obsługuje protokoły NEAR, RDP i Udostępnianie ekranu firmy Apple. Aby uzyskać więcej informacji, zobacz "Protokoły połączeń zdalnych" (s. 1078).

Funkcja pulpitu zdalnego umożliwia wykonywanie następujących zadań:

- Nawiązywanie połączenia z obciążeniami zdalnymi z systemem Windows, macOS i Linux przy użyciu protokołu NEAR w trybie Tylko do przeglądania.
- Nawiązywanie połączenia z obciążeniami zdalnymi z systemem Windows przy użyciu protokołu RDP.
- Nawiązywanie połączenia z obciążeniami zdalnymi z systemem macOS przy użyciu protokołu Udostępnianie ekranu firmy Apple w trybie Tylko do przeglądania lub Zasłona.
- Nawiązywanie połączenia z obciążeniami zarządzanymi i zdalne sterowanie nimi przy użyciu chmurowych połączeń zdalnych.
- Nawiązywanie połączenia z obciążeniami niezarządzanymi i zdalne sterowanie nimi przy użyciu bezpośrednich połączeń zdalnych.
- Nawiązywanie połączenia ze zdalnymi obciążeniami niezarządzanymi przy użyciu aplikacji Acronis Quick Assist.
- Nawiązywanie połączenia z obciążeniami zdalnymi przy użyciu różnych metod uwierzytelniania: za pomocą poświadczeń dostępu do obciążenia zdalnego, przy użyciu prośby o pozwolenie na obserwację lub sterowanie bądź przy użyciu kodu dostępu (w przypadku korzystania z aplikacji Quick Assist).
- Obserwowanie wielu monitorów naraz w trybie multiwidoku.
- Rejestrowanie sesji zdalnych (w ramach połączenia przy użyciu protokołu NEAR).
- Wyświetlanie raportu z historii sesji.

Dodatkowe informacje na temat funkcji wchodzących w skład pakietów Standardowy i Zarządzanie zaawansowane można znaleźć w sekcji "Obsługiwane funkcje pulpitu zdalnego i pomocy zdalnej" (s. 1074).

Funkcja pomocy zdalnej umożliwia wykonywanie następujących zadań:

- Nawiązywanie połączenia z obciążeniami zdalnymi z systemem Windows, macOS i Linux przy użyciu protokołu NEAR w trybie sterowania.
- Nawiązywanie połączenia z obciążeniami zdalnymi z systemem macOS przy użyciu protokołu Udostępnianie ekranu firmy Apple w trybie Sterowanie.
- Udzielanie pomocy zdalnej na obciążeniach przy użyciu chmurowych połączeń zdalnych.

© Acronis International GmbH, 2003-2024

- Przesyłanie plików między obciążeniem lokalnym a zdalnym.
- Wykonywanie podstawowych czynności z zakresu zarządzania na obciążeniu zdalnym, takich jak ponowne uruchomienie, zamknięcie systemu, uśpienie, opróżnienie kosza czy wylogowanie użytkownika zdalnego.
- Monitorowanie obciążenia zdalnego przez wykonywanie w pewnych odstępach zrzutów ekranu jego pulpitu.

Dodatkowe informacje na temat funkcji wchodzących w skład pakietów Ochrona standardowa i Zarządzanie zaawansowane można znaleźć w sekcji "Obsługiwane funkcje pulpitu zdalnego i pomocy zdalnej" (s. 1074).

Ważne
Aby aktywować wszystkie funkcje pulpitu zdalnego i pomocy zdalnej w przypadku obciążenia zarządzanego, trzeba skonfigurować plan zarządzania zdalnego i zastosować go do tego obciążenia. Chociaż na obciążeniu można zastosować tylko jeden plan zarządzania zdalnego, w zależności od potrzeb można skonfigurować różne plany zarządzania zdalnego i zastosować je do różnych obciążeń.

Można na przykład utworzyć plan zarządzania zdalnego, który ma włączony tylko protokół RDP, i zastosować go do części obciążeń. Dzięki temu będzie można nawiązywać połączenia zdalne z tymi obciążeniami bez aktywowania licencji pakietu Zarządzanie zaawansowane na każde obciążenie i bez dodatkowych opłat.

Z drugiej strony można utworzyć kolejny plan zarządzania zdalnego z włączonymi protokołami NEAR i Udostępnianie ekranu firmy Apple. W tym przypadku zostanie aktywowana licencja pakietu Zarządzanie zaawansowane na obciążenie i zostanie naliczona opłata za każde obciążenie, do którego zostanie zastosowany ten plan zarządzania zdalnego.

Dodatkowe informacje na temat planów zarządzania zdalnego i pracy z nimi można znaleźć w sekcji "Plany zarządzania zdalnego" (s. 1082).

© Acronis International GmbH, 2003-2024

Uwaga
Funkcje pulpitu zdalnego i pomocy zdalnej wymagają wykonania następujących zadań:

- Jednorazowa instalacja programu Klient rozwiązania Connect na obciążeniu zarządzającym (hoście). System zasugeruje pobranie klienta przy pierwszej próbie wykonania czynności zdalnej (sterowania zdalnego lub pomocy zdalnej) na obciążeniu docelowym. Program Klient rozwiązania Connect można też pobrać z poziomu okna **Do pobrania** w konsoli Ochrona. Dodatkowe informacje na temat ustawień, które można konfigurować, można znaleźć w sekcji "Konfigurowanie ustawień programu Klient rozwiązania Connect" (s. 1117).
- Instalacja modułu Agent rozwiązania Connect na obciążeniach zarządzanych. Agent rozwiązania Connect to moduł wchodzący w skład agenta Ochrona, począwszy od wersji 15.0.31266.
- W przypadku obciążeń zdalnych z systemem macOS należy przyznać modułowi Agent rozwiązania Connect wymagane uprawnienia systemowe. Aby uzyskać więcej informacji, zobacz "Instalowanie agentów ochrony w systemie macOS" (s. 89).
- Uruchomienie aplikacji Acronis Quick Assist na obciążeniach niezarządzanych. Można pobrać aplikację Acronis Quick Assist z witryny internetowej.

Dodatkowe informacje na temat platform obsługiwanych przez poszczególne komponenty pulpitu zdalnego i pomocy zdalnej można znaleźć w sekcji "Obsługiwane platformy" (s. 1077).

Obsługiwane funkcje pulpitu zdalnego i pomocy zdalnej

Poniższa tabela zawiera dodatkowe informacje na temat zmian w obsługiwanych funkcjach pulpitu zdalnego i pomocy zdalnej wprowadzonych w grudniu 2022 r.

Funkcja	Ochrona standardowa Przed grudniem 2022	Zarządzanie zaawansowane Przed grudniem 2022	Ochrona standardowa Po grudniu 2022	Zarządzanie zaawansowane Po grudniu 2022
Pomoc zdalna przy użyciu protokołu RDP w przypadku systemu Windows	Tak	Nie	Nie	Nie
Udostępnianie użytkownikom połączenia zdalnego	Nie	Tak	Nie	Nie
Połączenia zdalne				
Zdalnie wykonywane czynności	Nie	Nie	Tak	Tak
Wybieranie sesji do	Nie	Nie	Nie	Tak

© Acronis International GmbH, 2003-2024

Funkcja	Ochrona standardowa Przed grudniem 2022	Zarządzanie zaawansowane Przed grudniem 2022	Ochrona standardowa Po grudniu 2022	Zarządzanie zaawansowane Po grudniu 2022
połączenia w przypadku systemu Windows/macOS/Linux				
Połączenie bezpośrednie przy użyciu protokołów RDP i Udostępnianie ekranu firmy Apple	Nie	Nie	Nie	Tak
Sterowanie w wielu oknach	Nie	Nie	Nie	Tak
Tryby połączeń: Sterowanie / Tylko do przeglądania / Zasłona	Nie	Nie	Nie	Tak
Obsługa wspólnych poświadczeń na potrzeby połączeń zdalnych	Nie	Nie	Tak	Tak
Jednoczesne połączenia na technika				
przy użyciu protokołu RDP	Tak	Tak	Tak	Tak
przy użyciu protokołu NEAR	Nie	Nie	Nie	Tak
Przesyłanie i udostępnianie plików				
z systemu Windows do systemu Windows/macOS/Linux	Nie	Nie	Nie	Tak
z systemu macOS do systemu Windows/macOS/Linux	Nie	Nie	Nie	Tak
z systemu Linux do systemu	Nie	Nie	Nie	Tak

© Acronis International GmbH, 2003-2024

Funkcja	Ochrona standardowa Przed grudniem 2022	Zarządzanie zaawansowane Przed grudniem 2022	Ochrona standardowa Po grudniu 2022	Zarządzanie zaawansowane Po grudniu 2022
Windows/macOS/Linux				
Nawiązywanie połączeń przez aplikację Quick Assist				
z systemu Windows do systemu Windows/macOS/Linux	Nie	Nie	Nie	Tak
z systemu macOS do systemu Windows/macOS/Linux	Nie	Nie	Nie	Tak
z systemu Linux do systemu Windows/macOS/Linux	Nie	Nie	Nie	Tak
Połączenia zdalne przy użyciu protokołów				
Połączenie zdalne przy użyciu protokołu NEAR				
z systemu Windows do systemu Windows/macOS/Linux	Nie	Nie	Nie	Tak
z systemu macOS do systemu Windows/macOS/Linux	Nie	Nie	Nie	Tak
z systemu Linux do systemu Windows/macOS/Linux	Nie	Nie	Nie	Tak
Połączenie zdalne przy użyciu protokołu RDP (klient stacjonarny)				
z systemu Windows do systemu Windows	Tak	Tak	Tak	Tak
z systemu macOS do	Tak	Tak	Tak	Tak

© Acronis International GmbH, 2003-2024

Funkcja	Ochrona standardowa Przed grudniem 2022	Zarządzanie zaawansowane Przed grudniem 2022	Ochrona standardowa Po grudniu 2022	Zarządzanie zaawansowane Po grudniu 2022
systemu Windows				
z systemu Linux do systemu Windows	Nie	Nie	Tak	Tak
Połączenie zdalne przy użyciu protokołu RDP (klient internetowy)				
z systemu Windows do systemu Windows	Tak	Tak	Tak	Tak
z systemu macOS do systemu Windows	Tak	Tak	Tak	Tak
z systemu Linux do systemu Windows	Nie	Nie	Tak	Tak
Połączenie zdalne przy użyciu protokołu Udostępnianie ekranu firmy Apple				
z systemu Windows/macOS/Linux do systemu macOS	Nie	Nie	Nie	Tak
Zarządzanie sesjami				
Nagrywanie sesji	Nie	Nie	Nie	Tak
Raportowanie i monitorowanie				
Historia i przeszukiwanie sesji	Nie	Nie	Nie	Tak
Przesyłanie zrzutu ekranu	Nie	Nie	Nie	Tak

Obsługiwane platformy

W poniższej tabeli zestawiono systemy operacyjne obsługiwane przez poszczególne komponenty funkcji pulpitu zdalnego i pomocy zdalnej.

Komponent pulpitu zdalnego	Obsługiwane platformy
Klient rozwiązania Connect	• Windows 7 lub nowszy • macOS 10.13 lub nowszy • Linux: openSUSE 8

© Acronis International GmbH, 2003-2024

Komponent pulpitu zdalnego	Obsługiwane platformy
	Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Agent rozwiązania Connect	• Windows 7 lub nowszy • Windows Server 2008 R2 lub nowszy • macOS 10.13 lub nowszy • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) – 19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis Quick Assist	• Windows 7 lub nowszy • Windows Server 2008 R2 lub nowszy • macOS 10.13 lub nowszy • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) – 19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Protokoły połączeń zdalnych

Funkcja pulpitu zdalnego używa następujących protokołów do obsługi połączeń zdalnych.

NEAR

NEAR to opracowany przez firmę Acronis bardzo bezpieczny protokół, który można scharakteryzować następująco:

© Acronis International GmbH, 2003-2024

- ## H.264

  Protokół NEAR obejmuje trzy tryby jakości: **Płynny**, **Zrównoważony** i **Ostry**. W trybie **Płynny** protokół NEAR używa kodowania sprzętowego H.264 w systemach macOS i Windows do kodowania obrazu pulpitu, a w razie braku kodera sprzętowego wraca do kodera programowego. Rozmiar obrazu jest obecnie ograniczony do rozdzielczości Full HD (1920 x 1080).

- ## Koder-dekoder adaptacyjny

  W trybach jakości **Zrównoważony** i **Ostry** protokół NEAR używa kodera-dekodera adaptacyjnego, który zapewnia pełną jakość obrazu o 32-bitowej głębi — w porównaniu z trybem „wideo" stosowanym w standardzie H.264.

  W trybie **Zrównoważony** jakość obrazu jest automatycznie dostosowywana do aktualnych warunków w sieci i utrzymywana jest bieżąca liczba klatek na sekundę.

  W trybie **Ostry** obraz ma pełną jakość, ale jeśli sieć, procesor lub karta wideo są przeciążone, może być stosowana mniejsza liczba klatek na sekundę.

  Koder-dekoder adaptacyjny korzysta z technologii OpenCL w systemach Windows i macOS, gdy jest ona dostępna w sterownikach graficznych.

- ## Przesyłanie dźwięku

  Protokół NEAR obsługuje przechwytywanie dźwięku z komputera zdalnego i przesyłanie go do hosta. Dodatkowe informacje na temat włączania przekierowania dźwięku w ramach połączenia zdalnego w systemach Windows, macOS i Linux można znaleźć w sekcji "Przekierowanie dźwięku w ramach połączenia zdalnego" (s. 1080).

- ## Różne opcje logowania

  W celu zalogowania się na obciążeniu zdalnym możesz użyć następujących metod.

  Kod dostępu: użytkownik zalogowany na obciążeniu zdalnym uruchamia aplikację Quick Assist i podaje Ci kod dostępu. W przypadku tej metody zawsze jest nawiązywane połączenie z sesją aktualnie zalogowanego użytkownika.

  Poświadczenia dostępu do obciążenia: zaloguj się na obciążeniu zdalnym przy użyciu poświadczeń administratora zarejestrowanych na tym obciążeniu.

  Poproś o zgodę na obserwację lub sterowanie: użytkownik zalogowany na obciążeniu zdalnym zostanie poproszony o zezwolenie na połączenie lub odmowę połączenia.

- ## Zabezpieczenia

  W protokole NEAR Twoje dane są zawsze szyfrowane w dwóch kierunkach przy użyciu algorytmu szyfrowania AES.

© Acronis International GmbH, 2003-2024

RDP

Remote Desktop Protocol (RDP) to autorski protokół firmy Microsoft, który umożliwia łączenie się z komputerem zdalnym z systemem Windows przy użyciu połączenia sieciowego.

Udostępnianie ekranu firmy Apple

Udostępnianie ekranu firmy Apple to klient VNC firmy Apple dołączany do systemu macOS w wersji 10.5 i nowszych.

Przekierowanie dźwięku w ramach połączenia zdalnego

Program Klient rozwiązania Connect obsługuje strumieniowe przesyłanie dźwięku przy użyciu protokołu połączeń NEAR. Dodatkowe informacje na temat protokołu NEAR można znaleźć w sekcji "Protokoły połączeń zdalnych" (s. 1078).

Przekierowywanie dźwięku z obciążenia zdalnego z systemem Windows

W przypadku obciążeń z systemem Windows dźwięk zdalny powinien być przesyłany automatycznie. Upewnij się, że do obciążenia zdalnego są podłączone urządzenia wyjściowe dźwięku (głośniki lub słuchawki).

Przekierowywanie dźwięku z obciążenia zdalnego z systemem macOS

Aby włączyć przekierowywanie dźwięku z obciążenia z systemem macOS, upewnij się, że:

- Na obciążeniu jest zainstalowany agent Ochrona.
- Na obciążeniu jest zainstalowany sterownik przechwytywania dźwięku.
- Obciążenie używa do połączeń zdalnych protokołu NEAR.

Uwaga
W przypadku systemu macOS 10.15 Catalina trzeba przyznać programowi Agent rozwiązania Connect uprawnienie Mikrofon. Dodatkowe informacje na temat przyznawania programowi Agent rozwiązania Connect uprawnienia Mikrofon można znaleźć w sekcji "Przyznawanie wymaganych uprawnień systemowych modułowi Agent rozwiązania Connect" (s. 83).

Agent współpracuje z następującymi sterownikami przechwytywania dźwięku: Soundflower lub Blackhole.

Proces instalacji najnowszych wersji został opisany na stronie wiki sterownika Blackhole: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Uwaga
Program Klient rozwiązania Connect obsługuje obecnie tylko 2-kanałową wersję sterownika Blackhole.

© Acronis International GmbH, 2003-2024

Ewentualnie, jeśli na obciążeniu jest zainstalowany system zarządzania Homebrew, możesz zainstalować sterownik Blackhole, wykonując następujące polecenie:

```
brew install --cask blackhole-2ch
```

Uwaga
Dźwięk z obciążenia zdalnego z systemem macOS jest przekierowywany, ale użytkownik zalogowany na obciążeniu zdalnym nie będzie go słyszeć.

Przekierowywanie dźwięku z obciążenia zdalnego z systemem Linux

Przekierowanie dźwięku w ramach połączenia zdalnego powinno działać automatycznie w większości dystrybucji systemu Linux. Jeśli przekierowanie dźwięku zdalnego domyślnie nie działa, zainstaluj sterownik PulseAudio. W tym celu uruchom następujące polecenie:

```
sudo apt-get install pulseaudio
```

Połączenia z obciążeniami zdalnymi na potrzeby pulpitu zdalnego lub pomocy zdalnej

Funkcje pulpitu zdalnego i pomocy zdalnej udostępniają kilka sposobów nawiązywania bezpośrednich lub chmurowych połączeń zdalnych z obciążeniami.

Połączenia bezpośrednie są nawiązywane przy użyciu protokołu TCP/IP w sieci lokalnej (LAN) między programem Klient rozwiązania Connect a obciążeniem zdalnym, na którym nie zainstalowano agenta. Nie wymagają one dostępu do Internetu.

Połączenia chmurowe są nawiązywane między programem Klient rozwiązania Connect a agentem lub aplikacją Quick Assist na obciążeniu za pośrednictwem rozwiązania Acronis Cloud.

Poniższa tabela zawiera dodatkowe informacje na temat opcji połączeń chmurowych.

Połączenie chmurowe	Opcja Połączenie chmurowe	Tryb widoku	Obsługiwana czynność zdalna	Dostępność
przy użyciu protokołu NEAR	z programu Klient rozwiązania Connect do modułu Agent rozwiązania Connect z programu Klient rozwiązania Connect do modułu Quick Assist	Steruj Tylko do przeglądania	Pulpit zdalny Pomoc zdalna	obciążenia zarządzane
przy użyciu protokołu RDP	z programu Klient rozwiązania Connect do modułu Agent	Steruj	Pulpit zdalny	obciążenia zarządzane

© Acronis International GmbH, 2003-2024

Połączenie chmurowe	Opcja Połączenie chmurowe	Tryb widoku	Obsługiwana czynność zdalna	Dostępność
	rozwiązania Connect z klienta internetowego do modułu Agent rozwiązania Connect			
przez Udostępnianie ekranu firmy Apple	z programu Klient rozwiązania Connect do modułu Agent rozwiązania Connect	Steruj Tylko do przeglądania Zasłona	Pulpit zdalny Pomoc zdalna	obciążenia zarządzane

Poniższa tabela zawiera dodatkowe informacje na temat opcji połączeń bezpośrednich.

Połączenie bezpośrednie	Opcja Połączenie bezpośrednie	Obsługiwana czynność zdalna	Dostępność
przy użyciu protokołu RDP	z programu Klient rozwiązania Connect do serwera RDP	Pulpit zdalny	obciążenia niezarządzane
przez Udostępnianie ekranu firmy Apple	z programu Klient rozwiązania Connect do serwera Udostępniania ekranu firmy Apple	Pulpit zdalny Pomoc zdalna	obciążenia niezarządzane

Plany zarządzania zdalnego

Plany zarządzania zdalnego to plany, które stosuje się w przypadku agenta Ochrona, aby włączyć i skonfigurować funkcje pulpitu zdalnego i pomocy zdalnej na obciążeniach zarządzanych.

Jeśli do danego obciążenia nie zostanie zastosowany żaden plan zarządzania zdalnego, funkcje pulpitu zdalnego i pomocy zdalnej będą ograniczone do czynności zdalnych (ponowne uruchamianie, zamykanie systemu, usypianie, opróżnianie kosza i wylogowywanie użytkownika zdalnego).

Uwaga
Dostępność ustawień, które można skonfigurować w planie zarządzania zdalnego, zależy od dodatku Service Pack zastosowanego w przypadku danego dzierżawcy. Aby uzyskać dostęp do wszystkich ustawień, należy aktywować pakiet Zarządzanie zaawansowane. Dodatkowe informacje na temat funkcji wchodzących w skład pakietów Standardowy i Zarządzanie zaawansowane można znaleźć w sekcji "Obsługiwane funkcje pulpitu zdalnego i pomocy zdalnej" (s. 1074).

© Acronis International GmbH, 2003-2024

Tworzenie planu zarządzania zdalnego

Możesz utworzyć plan zarządzania zdalnego, a następnie przypisać go do obciążenia, aby skonfigurować funkcje pulpitu zdalnego i pomocy zdalnej na obciążeniu zarządzanym.

Uwaga
Dostępność ustawień planu zarządzania zdalnego zależy od limitu usługi przypisanego do dzierżawcy. Jeśli korzystasz z funkcji standardowych, możesz skonfigurować tylko połączenia przy użyciu protokołu RDP.

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby utworzyć plan zarządzania zdalnego

W sekcji Plany zarządzania zdalnego

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany zarządzania zdalnego**.
2. Utwórz plan zarządzania zdalnego przy użyciu jednej z dwóch opcji.
   - Jeśli na liście nie ma żadnych planów zarządzania zdalnego, kliknij **Utwórz**.
   - Jeśli na liście są plany zarządzania zdalnego, kliknij **Utwórz plan**.
3. [Opcjonalnie] Aby zmienić domyślną nazwę planu, kliknij ikonę ołówka, wpisz nazwę planu, a następnie kliknij **Kontynuuj**.
4. Kliknij **Protokoły połączenia** i włącz protokoły, które mają być dostępne w tym planie zarządzania zdalnego na potrzeby połączeń zdalnych: NEAR, RDP lub Udostępnianie ekranu firmy Apple.
5. [Opcjonalnie] W przypadku zastosowania protokołu NEAR w sekcji **Ustawienia zabezpieczeń** zaznacz lub wyczyść pola wyboru, aby włączyć lub wyłączyć odpowiednie ustawienia, a następnie kliknij **Gotowe**.

Ustawienie	Opis	Dostępność
Zablokuj obciążenie, gdy użytkownik się rozłączy z sesją konsoli	W przypadku wybrania tego ustawienia obciążenie zdalne zostanie zablokowane po rozłączeniu z sesją konsoli.	Windows, macOS
Zezwól tylko jednemu użytkownikowi na połączenie przez NEAR lub przesyłanie plików w danym czasie	W przypadku wybrania tego ustawienia operacje połączenia przy użyciu protokołu NEAR i przesyłania plików nie będą możliwe, dopóki będzie aktywne połączenie zdalne z	Windows, macOS, Linux

© Acronis International GmbH, 2003-2024

Ustawienie	Opis	Dostępność
	obciążeniem.	
Zezwól administratorowi obciążenia na połączenie z sesją dowolnego użytkownika niebędącego administratorem	W przypadku wybrania tego ustawienia administrator będzie mógł nawiązać połączenie z każdą standardową sesją użytkownika na obciążeniu. Jeśli zarówno opcja **Zezwól administratorowi obciążenia na połączenie z sesją dowolnego użytkownika niebędącego administratorem**, jak i opcja **Zezwól na tworzenie sesji systemowych** są wyczyszczone, możesz nawiązać połączenie tylko z aktywnymi sesjami administratora na obciążeniach zdalnych z systemem macOS.	Windows, macOS
Zezwól na tworzenie sesji systemowych	W przypadku wybrania tego ustawienia podczas nawiązywania połączeń zdalnych administrator będzie się łączyć w ramach nowej sesji, a nie jednej z już aktywnych sesji.	macOS
Zezwól na synchronizację schowka	W przypadku wybrania tego ustawienia będzie można przesyłać dane między swoim schowkiem a schowkiem obciążenia zdalnego. Na przykład będzie można skopiować jakiś tekst z pliku na obciążeniu zdalnym i wkleić go do pliku na własnym obciążeniu — i na odwrót.	Windows, macOS, Linux

6. Kliknij **Ustawienia zabezpieczeń**, zaznacz lub wyczyść pola wyboru, aby włączyć lub wyłączyć odpowiednie ustawienia, a następnie kliknij **Gotowe**.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
Pokaż, czy obciążenie jest zdalnie sterowane	W przypadku wybrania tego ustawienia na pulpicie obciążenia zdalnego zostanie wyświetlone powiadomienie, jeśli jest aktywne połączenie pulpitu zdalnego z tym obciążeniem.
Poproś użytkownika o zgodę na wykonanie zrzutów ekranu obciążenia	W przypadku wybrania tego ustawienia użytkownik obciążenia zdalnego otrzyma powiadomienie, gdy administrator poprosi o przesyłanie zrzutów ekranu z tego obciążenia.

7. Kliknij **Zarządzanie obciążeniami**, wybierz funkcje, które mają być dostępne na obciążeniach zdalnych, a następnie kliknij **Gotowe**.

Ustawienie	Opis	Dostępność
Przesyłanie plików	Umożliwia przesyłanie plików między obciążeniami lokalnymi i zdalnymi.	Windows, macOS, Linux
Przesyłanie zrzutu ekranu	Umożliwia przesyłanie zrzutów ekranu pulpitu obciążenia zdalnego do konsoli Cyber Protect.	Windows, macOS, Linux

8. Kliknij **Ustawienia wyświetlania**, zaznacz lub wyczyść pola wyboru, aby włączyć lub wyłączyć odpowiednie ustawienia, a następnie kliknij **Gotowe**.

Uwaga
Sekcja **Ustawienia wyświetlania** jest dostępna tylko w przypadku połączeń przy użyciu protokołu NEAR.

Ustawienie	Opis	Dostępność
Użyj funkcji powielania pulpitu w celu przechwycenia obrazu pulpitu	Powielanie pulpitu jest jedną z metod przechwytywania ekranu w systemie Windows. W niektórych środowiskach może ona być niestabilna. Jeśli nie skorzystasz z powielania pulpitu, będziesz zamiast niego używać podstawowej metody (BitBlt) — jest ona znacznie wolniejsza, ale bardziej	Windows

© Acronis International GmbH, 2003-2024

Ustawienie	Opis	Dostępność
	stabilna.	
Użyj funkcji przyspieszenia OpenCL	Przyspieszenie OpenCL może zwiększyć szybkość działania kodera-dekodera adaptacyjnego, który odpowiada za tryb jakości **Zrównoważony**, dzięki wykonywaniu części operacji obliczeniowych przez procesor graficzny (graphics processing unit, GPU). Wymaga to instalacji sterownika OpenCL w zdalnym systemie Linux. Koder-dekoder adaptacyjny korzysta z technologii OpenCL w systemach macOS i Windows, gdy jest ona dostępna w sterownikach graficznych.	Linux
Użyj funkcji kodowania sprzętowego H.264	Protokół NEAR obsługuje trzy tryby jakości: **Płynny**, **Zrównoważony** i **Ostry**. W przypadku trybu **Płynny** obraz pulpitu jest kodowany przy użyciu kodowania sprzętowego H.264. W trybie **Zrównoważony** używany jest koder-dekoder adaptacyjny, który zapewnia pełną jakość obrazu o 32-bitowej głębi — w porównaniu z trybem „wideo" stosowanym w standardzie H.264. Jakość obrazu jest automatycznie dostosowywana do aktualnych warunków w sieci i utrzymywana jest bieżąca liczba klatek na sekundę. W trybie **Ostry** używany jest koder-dekoder adaptacyjny,	Windows, macOS

© Acronis International GmbH, 2003-2024

Ustawienie	Opis	Dostępność
	który zapewnia pełną jakość obrazu o 32-bitowej głębi — w porównaniu z trybem „wideo” stosowanym w standardzie H.264. Obraz ma zawsze pełną jakość, ale w przypadku przeciążenia sieci lub procesora / karty wideo może być stosowana mniejsza liczba klatek na sekundę.	

9. Jeśli chcesz, aby w szczegółach obciążeń były widoczne informacje o ostatnio zalogowanych na nich użytkownikach, kliknij **Przybornik**, zaznacz **Pokaż ostatnio zalogowanych użytkowników**, a następnie kliknij **Gotowe**.

   Dodatkowe informacje na temat ostatnio zalogowanych użytkowników można znaleźć w sekcji "Znajdź ostatniego zalogowanego użytkownika" (s. 390).
10. [Opcjonalnie] Aby dodać obciążenia do planu:
    a. Kliknij **Dodaj obciążenia**.
    b. Wybierz obciążenia, a następnie kliknij **Dodaj**.
    c. Jeśli występują problemy z kompatybilnością, które chcesz rozwiązać, wykonaj procedurę opisaną w sekcji "Rozwiązywanie problemów z kompatybilnością z planami zarządzania zdalnego" (s. 1096).
11. Kliknij **Utwórz**.

W sekcji Wszystkie urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie, do którego chcesz zastosować plan zarządzania zdalnego.
3. Kliknij **Chroń**, a następnie kliknij **Dodaj plan**.
4. Kliknij **Utwórz plan** i wybierz **Zarządzanie zdalne**.
5. [Opcjonalnie] Aby zmienić domyślną nazwę planu, kliknij ikonę ołówka, wpisz nazwę planu, a następnie kliknij **Kontynuuj**.
6. Kliknij **Protokoły połączenia** i włącz protokoły, które mają być dostępne w tym planie zarządzania zdalnego na potrzeby połączeń zdalnych: NEAR, RDP lub Udostępnianie ekranu firmy Apple.
7. [Opcjonalnie] W przypadku zastosowania protokołu NEAR w sekcji **Ustawienia zabezpieczeń** zaznacz lub wyczyść pola wyboru, aby włączyć lub wyłączyć odpowiednie ustawienia, a następnie kliknij **Gotowe**.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis	Dostępność
Zablokuj obciążenie, gdy użytkownik się rozłączy z sesją konsoli	W przypadku wybrania tego ustawienia obciążenie zdalne zostanie zablokowane po rozłączeniu z sesją konsoli.	Windows, macOS
Zezwól tylko jednemu użytkownikowi na połączenie przez NEAR lub przesyłanie plików w danym czasie	W przypadku wybrania tego ustawienia operacje połączenia przy użyciu protokołu NEAR i przesyłania plików nie będą możliwe, dopóki będzie aktywne połączenie zdalne z obciążeniem.	Windows, macOS, Linux
Zezwól administratorowi obciążenia na połączenie z sesją dowolnego użytkownika niebędącego administratorem	W przypadku wybrania tego ustawienia administrator będzie mógł nawiązać połączenie z każdą standardową sesją użytkownika na obciążeniu. Jeśli zarówno opcja **Zezwól administratorowi obciążenia na połączenie z sesją dowolnego użytkownika niebędącego administratorem**, jak i opcja **Zezwól na tworzenie sesji systemowych** są wyczyszczone, możesz nawiązać połączenie tylko z aktywnymi sesjami administratora na obciążeniach zdalnych z systemem macOS.	Windows, macOS
Zezwól na tworzenie sesji systemowych	W przypadku wybrania tego ustawienia podczas nawiązywania połączeń zdalnych administrator będzie się łączyć w ramach nowej sesji, a nie jednej z już aktywnych sesji.	macOS
Zezwól na synchronizację schowka	W przypadku wybrania tego ustawienia będzie można	Windows, macOS, Linux

© Acronis International GmbH, 2003-2024

Ustawienie	Opis	Dostępność
	przesyłać dane między swoim schowkiem a schowkiem obciążenia zdalnego. Na przykład będzie można skopiować jakiś tekst z pliku na obciążeniu zdalnym i wkleić go do pliku na własnym obciążeniu — i na odwrót.	

8. Kliknij **Ustawienia zabezpieczeń**, zaznacz lub wyczyść pola wyboru, aby włączyć lub wyłączyć odpowiednie ustawienia, a następnie kliknij **Gotowe**.

Ustawienie	Opis
Pokaż, czy obciążenie jest zdalnie sterowane	W przypadku wybrania tego ustawienia na pulpicie obciążenia zdalnego zostanie wyświetlone powiadomienie, jeśli jest aktywne połączenie pulpitu zdalnego z tym obciążeniem.
Poproś użytkownika o zgodę na wykonanie zrzutów ekranu obciążenia	W przypadku wybrania tego ustawienia użytkownik obciążenia zdalnego otrzyma powiadomienie, gdy administrator poprosi o przesyłanie zrzutów ekranu z tego obciążenia.

9. Kliknij **Zarządzanie obciążeniami**, wybierz funkcje, które mają być dostępne na obciążeniach zdalnych, a następnie kliknij **Gotowe**.

Ustawienie	Opis	Dostępność
Przesyłanie plików	Umożliwia przesyłanie plików między obciążeniami lokalnymi i zdalnymi.	Windows, macOS, Linux
Przesyłanie zrzutu ekranu	Umożliwia przesyłanie zrzutów ekranu pulpitu obciążenia zdalnego do konsoli Cyber Protect.	Windows, macOS, Linux

10. Kliknij **Ustawienia wyświetlania**, zaznacz lub wyczyść pola wyboru, aby włączyć lub wyłączyć odpowiednie ustawienia, a następnie kliknij **Gotowe**.

Uwaga
Sekcja **Ustawienia wyświetlania** jest dostępna tylko w przypadku połączeń przy użyciu protokołu NEAR.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis	Dostępność
Użyj funkcji powielania pulpitu w celu przechwycenia obrazu pulpitu	Powielanie pulpitu jest jedną z metod przechwytywania ekranu w systemie Windows. W niektórych środowiskach może ona być niestabilna. Jeśli nie skorzystasz z powielania pulpitu, będziesz zamiast niego używać podstawowej metody (BitBlt) — jest ona znacznie wolniejsza, ale bardziej stabilna.	Windows
Użyj funkcji przyspieszenia OpenCL	Przyspieszenie OpenCL może zwiększyć szybkość działania kodera-dekodera adaptacyjnego, który odpowiada za tryb jakości **Zrównoważony**, dzięki wykonywaniu części operacji obliczeniowych przez procesor graficzny (graphics processing unit, GPU). Wymaga to instalacji sterownika OpenCL w zdalnym systemie Linux. Koder-dekoder adaptacyjny korzysta z technologii OpenCL w systemach macOS i Windows, gdy jest ona dostępna w sterownikach graficznych.	Linux
Użyj funkcji kodowania sprzętowego H.264	Protokół NEAR obsługuje trzy tryby jakości: **Płynny**, **Zrównoważony** i **Ostry**. W przypadku trybu **Płynny** obraz pulpitu jest kodowany przy użyciu kodowania sprzętowego H.264. W trybie **Zrównoważony** używany jest koder-dekoder adaptacyjny, który zapewnia pełną jakość obrazu o 32-bitowej głębi — w	Windows, macOS

© Acronis International GmbH, 2003-2024

Ustawienie	Opis	Dostępność
	porównaniu z trybem „wideo” stosowanym w standardzie H.264. Jakość obrazu jest automatycznie dostosowywana do aktualnych warunków w sieci i utrzymywana jest bieżąca liczba klatek na sekundę. W trybie **Ostry** używany jest koder-dekoder adaptacyjny, który zapewnia pełną jakość obrazu o 32-bitowej głębi — w porównaniu z trybem „wideo” stosowanym w standardzie H.264. Obraz ma zawsze pełną jakość, ale w przypadku przeciążenia sieci lub procesora / karty wideo może być stosowana mniejsza liczba klatek na sekundę.	

11. Jeśli chcesz, aby w szczegółach obciążeń były widoczne informacje o ostatnio zalogowanych na nich użytkownikach, kliknij **Przybornik**, zaznacz **Pokaż ostatnio zalogowanych użytkowników**, a następnie kliknij **Gotowe**.
    Dodatkowe informacje na temat ostatnio zalogowanych użytkowników można znaleźć w sekcji "Znajdź ostatniego zalogowanego użytkownika" (s. 390).
12. Kliknij **Utwórz**.

Dodawanie obciążenia do planu zarządzania zdalnego

W zależności od potrzeb po utworzeniu planu zarządzania zdalnego można do niego dodać obciążenia.

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby dodać obciążenie do planu zarządzania zdalnego

W sekcji Plany zarządzania zdalnego

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany zarządzania zdalnego**.
2. Kliknij plan zarządzania zdalnego.

© Acronis International GmbH, 2003-2024

3. W zależności od tego, czy plan został już zastosowany do jakiegoś obciążenia, wykonaj następujące czynności:
   - Kliknij **Dodaj obciążenia**, jeśli plan nie został jeszcze zastosowany do żadnego obciążenia.
   - Kliknij **Zarządzaj obciążeniami**, jeśli plan nie został jeszcze zastosowany do żadnego obciążenia.
4. Wybierz obciążenie z listy i kliknij **Dodaj**.
5. Kliknij **Zapisz**.
6. Kliknij **Potwierdź**, aby zastosować do obciążenia wymagany limit usługi.

W sekcji Wszystkie urządzenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie, do którego chcesz zastosować plan zarządzania zdalnego.
3. Kliknij **Chroń**, a następnie kliknij **Dodaj plan**.
4. W sekcji **Wybierz plan z poniższej listy** wybierz **Zarządzanie zdalne**, aby wyświetlić tylko plany zarządzania zdalnego.
5. Kliknij **Zastosuj**.
6. Kliknij **Potwierdź**, aby zastosować do obciążenia wymagany limit usługi.

Usuwanie obciążeń z planu zarządzania zdalnego

W zależności od potrzeb można usunąć obciążenia z planu zarządzania zdalnego.

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby usunąć obciążenia z planu zarządzania zdalnego

1. W konsoli Cyber Protect przejdź do sekcji **Zarządzanie** > **Plany zarządzania zdalnego**.
2. Kliknij plan zarządzania zdalnego.
3. Kliknij **Zarządzaj obciążeniami**.
4. Wybierz co najmniej jedno obciążenie, które chcesz usunąć z planu zarządzania zdalnego, a następnie kliknij **Usuń**.
5. Kliknij **Gotowe**.
6. Kliknij **Zapisz**.

Dodatkowe czynności w ramach istniejących już planów zarządzania zdalnego

Na ekranie **Plany zarządzania zdalnego** możesz wykonywać następujące dodatkowe czynności związane z planami zarządzania zdalnego: wyświetlanie szczegółów, edytowanie, wyświetlanie

© Acronis International GmbH, 2003-2024

działań, wyświetlanie alertów, zmienianie nazwy, włączanie, wyłączanie, klonowanie, eksportowanie, ustawianie jako ulubione, ustawianie jako domyślne i usuwanie.

Wyświetl szczegóły

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby wyświetlić szczegóły planu zarządzania zdalnego

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Wyświetl szczegóły**.

Edytuj

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby edytować plan

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Edytuj**.

Działania

Aby wyświetlić działania dotyczące planu zarządzania zdalnego

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Działania**.
3. Kliknij działanie, aby wyświetlić więcej informacji na jego temat.

Alerty

Aby wyświetlić alerty

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Alerty**.

Zmień nazwę

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby zmienić nazwę planu zarządzania zdalnego

© Acronis International GmbH, 2003-2024

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Zmień nazwę**.
3. Wprowadź nową nazwę planu, a następnie kliknij **Kontynuuj**.

Włącz

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby włączyć plan zarządzania zdalnego

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Włącz**.

Wyłącz

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby wyłączyć plan zarządzania zdalnego

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Wyłącz**.

Klonuj

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby sklonować plan zarządzania zdalnego

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Klonuj**.
3. Kliknij **Utwórz**.

Eksportuj

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby wyeksportować plan zarządzania zdalnego

© Acronis International GmbH, 2003-2024

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Eksportuj**.
   Konfiguracja planu zostanie wyeksportowana na komputer lokalny w formacie JSON.

Ustaw jako domyślne

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby ustawić plan zarządzania zdalnego jako domyślny

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Ustaw jako domyślne**.
3. W oknie potwierdzenia kliknij **Ustaw**.
   Na ekranie **Plany zdalnego zarządzania** obok nazwy planu jest widoczny znacznik **Domyślne**.

Ustaw jako ulubione

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby ustawić plan zarządzania zdalnego jako ulubiony

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Dodaj do ulubionych**.
   Na ekranie **Plany zarządzania zdalnego** obok nazwy będzie widoczna ikona gwiazdki.

Usuń

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby usunąć plan zarządzania zdalnego

1. Na ekranie **Plany zarządzania zdalnego** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu zarządzania zdalnego.
2. Kliknij **Usuń**.
3. Wybierz **Potwierdzam**, a następnie kliknij **Usuń**.

Problemy z kompatybilnością z planami zarządzania zdalnego

W niektórych przypadkach zastosowanie planu zarządzania zdalnego na obciążeniu może spowodować problemy z kompatybilnością. Można zauważyć następujące problemy z

© Acronis International GmbH, 2003-2024

kompatybilnością:

- Konflikt planów — ten problem występuje, gdy na obciążeniu został już zastosowany inny plan zarządzania zdalnego, ponieważ na obciążeniu można zastosować tylko jeden plan zarządzania zdalnego.
- Niekompatybilny system operacyjny — ten problem jest powodowany nieobsługiwanym systemem operacyjnym obciążenia.
- Nieobsługiwany agent — ten problem występuje, gdy na obciążeniu znajduje się agent ochrony w przestarzałej wersji, który nie obsługuje funkcji pulpitu zdalnego.
- Za mały limit — ten problem występuje, gdy dzierżawca ma zbyt mały limit usługi, aby można było ją przypisać do wybranych obciążeń.

Jeśli plan zarządzania zdalnego jest stosowany do maksymalnie 150 indywidualnie wybranych obciążeń, zostanie wyświetlony monit o rozwiązanie istniejących konfliktów przed zapisaniem planu. Aby rozwiązać konflikt, wyeliminuj jego główną przyczynę lub usuń z planu obciążenia, których dotyczy ten konflikt. Aby uzyskać więcej informacji, zobacz "Rozwiązywanie problemów z kompatybilnością z planami zarządzania zdalnego" (s. 1096). W przypadku zapisania planu bez rozwiązania konfliktów zostanie on automatycznie wyłączony dla niekompatybilnych obciążeń i zostaną wyświetlone alerty.

Jeśli plan zarządzania zdalnego jest stosowany do więcej niż 150 obciążeń lub do grup urządzeń, najpierw zostanie zapisany, a następnie sprawdzony pod kątem kompatybilności. Plan ten zostanie automatycznie wyłączony dla niekompatybilnych obciążeń i zostaną wyświetlone alerty.

Rozwiązywanie problemów z kompatybilnością z planami zarządzania zdalnego

W zależności od przyczyny problemów z kompatybilnością można wykonać różne czynności w celu rozwiązania problemów z kompatybilnością w ramach procesu tworzenia nowego planu zarządzania zdalnego.

Uwaga
W przypadku rozwiązywania problemu ze zgodnością przez usunięcie obciążeń z planu nie można usunąć obciążeń należących do grupy urządzeń.

Aby rozwiązać problemy z kompatybilnością

1. Kliknij **Przejrzyj problemy**.
2. [Aby rozwiązać problemy z kompatybilnością z istniejącymi już planami zarządzania zdalnego przez usunięcie obciążeń z nowego planu]
   a. Na karcie **Plany powodujące konflikt** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.

© Acronis International GmbH, 2003-2024

3. [Aby rozwiązać problemy z kompatybilnością z planami zarządzania zdalnego przez wyłączenie planów już zastosowanych na obciążeniach]
   a. Kliknij **Wyłącz zastosowane plany**.
   b. Kliknij **Wyłącz**, a następnie kliknij **Zamknij**.
4. [Aby rozwiązać problemy z kompatybilnością spowodowane przez niekompatybilne systemy operacyjne]
   a. Na karcie **Niekompatybilny system operacyjny** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
5. [Aby rozwiązać problemy z kompatybilnością spowodowane przez nieobsługiwane agenty, usuwając obciążenia z planu]
   a. Na karcie **Nieobsługiwane agenty** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
6. [Aby rozwiązać problemy z kompatybilnością spowodowane przez nieobsługiwane agenty, aktualizując wersje agentów] Kliknij **Przejdź do listy agentów**.

   Uwaga
   Ta opcja jest dostępna wyłącznie dla administratorów klientów.

7. [Aby rozwiązać problemy z kompatybilnością spowodowane za małym limitem przez usunięcie obciążeń z planu]
   a. Na karcie **Za mały limit** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
8. [Aby rozwiązać problemy ze zgodnością spowodowane za małym limitem przez zwiększenie limitu dzierżawcy]

   Uwaga
   Ta opcja jest dostępna wyłącznie dla administratorów partnerów.

   a. Na karcie **Za mały limit** kliknij **Przejdź do portalu zarządzania**.
   b. Zwiększ limit usługi dla klienta.

Poświadczenia dostępu do obciążenia

Możesz dodać poświadczenia (nazwę użytkownika i hasło lub hasło VNC) użytkownika będącego administratorem obciążenia zdalnego lub nim niebędącego, zapisać je w magazynie poświadczeń w chmurze, a następnie użyć ich do automatycznego uwierzytelniania podczas nawiązywania połączenia z obciążeniami, którymi zarządzasz. Dzięki temu nie trzeba będzie wprowadzać tych

© Acronis International GmbH, 2003-2024

poświadczeń ręcznie za każdym razem podczas uwierzytelniania połączenia — wystarczy raz zapisać je w magazynie poświadczeń i przypisać do wielu obciążeń, a wówczas program Klient rozwiązania Connect użyje ich za każdym razem, gdy zechcesz połączyć się zdalnie z tymi obciążeniami.

Uwaga
Poświadczenia przechowywane w magazynie poświadczeń nie są udostępniane między różnymi poziomami dzierżawców. Są udostępniane tylko na tym samym poziomie dzierżawcy dla tego samego dzierżawcy-klienta lub dzierżawcy-partnera.

Oznacza to, że jeśli dzierżawca-klient ma kilku administratorów, będą oni widzieć poświadczenia w magazynie poświadczeń i będą mogli je współdzielić, podczas gdy inni administratorzy partnerów lub administratorzy klientów innych dzierżawców nie będą widzieć tych poświadczeń ani nie będą mogli z nich korzystać.

Dodawanie poświadczeń

Możesz dodać poświadczenia, a następnie używać ich do połączeń zdalnych z wieloma obciążeniami.

Aby dodać poświadczenia do obciążenia i je zapisać w magazynie poświadczeń

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie, dla którego chcesz dodać poświadczenia.
3. Dostęp do menu **Ustawienia** można uzyskać w jeden z następujących sposobów:
   - Kliknij **Pulpit zdalny**, a następnie kliknij **Ustawienia**.
   - Kliknij **Zarządzaj**, a następnie kliknij **Ustawienia**.
4. Kliknij **Dodaj poświadczenia**.
5. W obszarze **Magazyn poświadczeń** kliknij **Dodaj poświadczenia**.
6. Wprowadź poświadczenia.

Pole	Opis
Nazwa poświadczenia	Identyfikator poświadczeń, który będzie wyświetlany w magazynie poświadczeń.
Nazwa użytkownika	Nazwa użytkownika, która będzie używana do połączeń zdalnych z obciążeniem docelowym.
Hasło	Hasło, które będzie używane do połączeń zdalnych z obciążeniem docelowym.
Hasło VNC	To pole jest dostępne tylko w przypadku korzystania z aplikacji Udostępnianie ekranu firmy Apple.

7. Kliknij **Zapisz**.

© Acronis International GmbH, 2003-2024

Przypisywanie poświadczeń do obciążenia

Po dodaniu poświadczeń możesz ich używać do automatycznego uwierzytelniania podczas nawiązywania połączenia z zarządzanym przez siebie obciążeniem.

Aby przypisać zapisane poświadczenia do obciążenia na potrzeby automatycznego uwierzytelniania

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Dostęp do menu **Ustawienia** można uzyskać w jeden z następujących sposobów:
   - Kliknij **Pulpit zdalny**, a następnie kliknij **Ustawienia**.
   - Kliknij **Zarządzaj**, a następnie kliknij **Ustawienia**.
3. Na karcie obsługiwanego protokołu (NEAR, RDP lub Udostępnianie ekranu firmy Apple) kliknij **Dodaj poświadczenia**.
4. W obszarze **Magazyn poświadczeń** wybierz poświadczenia z listy, a następnie kliknij **Wybierz poświadczenia**.

Usuwanie poświadczeń

Niepotrzebne już poświadczenia można usunąć.

Aby usunąć poświadczenia z magazynu poświadczeń

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Dostęp do menu **Ustawienia** można uzyskać w jeden z następujących sposobów:
   - Kliknij **Pulpit zdalny**, a następnie kliknij **Ustawienia**.
   - Kliknij **Zarządzaj**, a następnie kliknij **Ustawienia**.
3. Na karcie obsługiwanego protokołu (NEAR, RDP lub Udostępnianie ekranu firmy Apple) kliknij **Usuń**.
4. W oknie z monitem o potwierdzenie kliknij **Usuń**.

Cofanie przypisania poświadczeń z obciążenia

Możesz cofnąć przypisanie poświadczeń z obciążenia, ale zachować je w magazynie poświadczeń.

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Dostęp do menu **Ustawienia** można uzyskać w jeden z następujących sposobów:
   - Kliknij **Pulpit zdalny**, a następnie kliknij **Ustawienia**.
   - Kliknij **Zarządzaj**, a następnie kliknij **Ustawienia**.
3. Na karcie obsługiwanego protokołu (NEAR, RDP lub Udostępnianie ekranu firmy Apple) kliknij **Cofnij przypisanie**.
4. W oknie z monitem o potwierdzenie kliknij **Cofnij przypisanie**.

© Acronis International GmbH, 2003-2024

Praca z obciążeniami zarządzanymi

Obciążenia zarządzane to obciążenia, na których jest zainstalowany agent Ochrona.

Na zarządzanych obciążeniach zdalnych można wykonywać następujące czynności:

- Nawiązywanie połączeń na potrzeby pomocy zdalnej lub pulpitu zdalnego przy użyciu protokołu NEAR w trybie Sterowanie lub Tylko do przeglądania
- Nawiązywanie połączeń na potrzeby pulpitu zdalnego przy użyciu protokołu RDP w trybie sterowania
- Nawiązywanie połączeń na potrzeby pomocy zdalnej lub połączeń pulpitu zdalnego przy użyciu protokołu Udostępnianie ekranu firmy Apple w trybie Sterowanie, Tylko do przeglądania lub Zasłona
- Nawiązywanie połączeń na potrzeby pulpitu zdalnego przy użyciu klienta internetowego
- Ponowne uruchamianie, zamykanie systemu, usypianie, opróżnienie kosza, wyloguj użytkownika zdalnego z obciążenia zdalnego
- Przesyłanie plików między własnym obciążeniem a obciążeniami zdalnymi
- Monitorowanie obciążeń zdalnych dzięki wykonywaniu zrzutów ekranu

Uwaga
Połączenia pulpitu zdalnego z obciążeniami zarządzanymi wymagają zainstalowania agenta Ochrona i zastosowania planu zarządzania zdalnego na obciążeniu.

Konfigurowanie ustawień protokołu RDP

Możesz skonfigurować ustawienia, które będą automatycznie stosowane do połączeń RDP w trybie zdalnego sterowania nawiązywanych z obciążeniem zarządzanym.

Aby skonfigurować ustawienia protokołu RDP obciążenia

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Dostęp do menu **Ustawienia** można uzyskać w jeden z następujących sposobów:
   - Kliknij **Pulpit zdalny**, a następnie kliknij **Ustawienia**.
   - Kliknij **Zarządzaj**, a następnie kliknij **Ustawienia**.

© Acronis International GmbH, 2003-2024

3. Skonfiguruj ustawienia dostępne na karcie **RDP**.

Ustawienie	Opis
Odtwarzanie dźwięku	To ustawienie umożliwia włączanie lub wyłączanie przekierowania dźwięku obciążenia zdalnego na obciążenie lokalne.
Nagrywanie dźwięku	To ustawienie umożliwia określenie, czy nagrywanie dźwięku (wypowiedzi do mikrofonu) będzie przekazywane do obciążenia zdalnego.
Przekierowuj drukarki	W przypadku wybrania tego ustawienia drukarki z danego obciążenia będą dostępne na obciążeniu zdalnym.
Przekierowuj pliki	To ustawienie umożliwia określenie, czy pliki z obciążenia lokalnego będą udostępniane obciążeniu zdalnemu.
Głębia kolorów	To ustawienie umożliwia określenie liczby kolorów w obrazie przesyłanym przez RDP. Wyższa wartość wymaga większej przepustowości łącza. **High Color**: głębia 16-bitowa **True Color**: • głębia 24-bitowa w przypadku połączeń przy użyciu protokołu RDP wykonywanych za pośrednictwem klienta internetowego • głębia 32-bitowa w przypadku połączeń przy użyciu protokołu RDP wykonywanych za pośrednictwem programu Klient rozwiązania Connect

4. Kliknij przycisk Zamknij.

Nawiązywanie połączeń z obciążeniami zarządzanymi na potrzeby pulpitu zdalnego lub pomocy zdalnej

Uwaga
Dostępność protokołów połączeń, których można używać do połączeń zdalnych, zależy od konfiguracji planu zarządzania zdalnego oraz od systemu operacyjnego obciążenia zdalnego.

Wymagania wstępne

- Na obciążeniu zarządzanym jest stosowany plan zarządzania zdalnego z włączonym odpowiednim protokołem połączeń.
- Obciążenie ma przypisany wymagany limit usługi. (Limit usługi jest uzyskiwany automatycznie po zastosowaniu do obciążenia planu zarządzania zdalnego).
- [W przypadku połączeń przy użyciu aplikacji Udostępnianie ekranu firmy Apple] Na obciążeniu z systemem macOS jest włączona opcja Udostępnianie ekranu firmy Apple.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.

© Acronis International GmbH, 2003-2024

Aby nawiązać połączenie zdalne z obciążeniem zarządzanym na potrzeby pulpitu zdalnego lub pomocy zdalnej

1. W konsoli Cyber Protect kliknij kolejno **Urządzenia** > **Komputery z agentami**.
2. Kliknij obciążenie, z którym chcesz nawiązać połączenie.
3. Kliknij **Pulpit zdalny**.
   Domyślnie jako protokół połączenia jest wybrany protokół NEAR.
4. [Opcjonalnie] Z listy rozwijanej **Protokół połączenia** wybierz protokół połączenia, którego chcesz użyć.
5. Kliknij tryb widoku, którego chcesz użyć.

Protokół	Połączenia zdalne z	Tryb widoku	Obsługiwana czynność zdalna
NEAR	Windows Linux macOS	**Steruj** — w tym trybie można obserwować i wykonywać operacje na obciążeniu zdalnym. **Tylko do przeglądania** — w tym trybie można tylko obserwować obciążenie zdalne.	Pulpit zdalny Pomoc zdalna
RDP	Windows	**Steruj** — w tym trybie można wyświetlać i wykonywać operacje na obciążeniu zdalnym. **Uwaga** Jeśli protokół RDP jest wyłączony w ustawieniach systemu operacyjnego obciążenia, pojawi się wyskakujące okienko. Skorzystaj z niego, aby włączyć protokół RDP dla obciążenia w ramach bieżącej sesji lub ogólnie: • Jeśli chcesz włączyć protokół RDP dla tego obciążenia tylko w ramach bieżącej sesji, zaznacz opcję **Wyłącz po zakończeniu sesji**, a następnie kliknij **Pozwól**. • Jeśli chcesz włączyć protokół RDP dla tego obciążenia, kliknij przycisk **Pozwól**.	Pulpit zdalny
Udostępnianie ekranu firmy Apple	macOS	**Steruj** — w tym trybie można obserwować i wykonywać operacje na obciążeniu zdalnym. **Tylko do przeglądania** — w tym	Pulpit zdalny Pomoc zdalna

© Acronis International GmbH, 2003-2024

Protokół	Połączenia zdalne z	Tryb widoku	Obsługiwana czynność zdalna
		trybie można tylko obserwować obciążenie zdalne. **Zasłona** — tryb dostępny tylko w przypadku obciążeń z systemem macOS. Jeśli połączenie z obciążeniem zdalnym zostanie nawiązane w trybie zasłony, wyświetlacz obciążenia zdalnego zostanie przyciemniony i użytkownik zdalny nie będzie widzieć, co robisz na obciążeniu.	

6. W zależności od tego, czy na obciążeniu jest zainstalowany program Klient rozwiązania Connect, wykonaj jedną z następujących czynności:
   - Jeśli program Klient rozwiązania Connect nie jest zainstalowany, pobierz go, zainstaluj, a następnie w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Pozwól**.
   - Jeśli program Klient rozwiązania Connect jest już zainstalowany, w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Otwórz klienta rozwiązania Connect**.
7. W oknie **Uwierzytelnianie** wybierz opcję uwierzytelniania, a następnie wpisz wymagane poświadczenia.

Uwaga
Jeśli do obciążenia zostały przypisane poświadczenia, uwierzytelnianie zostanie przeprowadzone automatycznie i ten krok zostanie pominięty. Aby uzyskać więcej informacji, zobacz "Przypisywanie poświadczeń do obciążenia" (s. 1099).

Opcja uwierzytelniania	Opis
Przy użyciu poświadczeń dostępu do obciążenia zdalnego	Połączenie zdalne będzie można nawiązać po podaniu nazwy użytkownika i hasła administratora na obciążeniu zdalnym. Ta opcja jest dostępna w przypadku protokołów NEAR, RDP i Udostępnianie ekranu firmy Apple. Z tej możliwości można skorzystać w celu uwierzytelnienia na potrzeby pulpitu zdalnego i pomocy zdalnej.
Poproś o zgodę na obserwację	Połączenie zdalne będzie można nawiązać w trybie obserwacji po uzyskaniu zezwolenia od użytkownika zalogowanego na obciążeniu zdalnym. Ta opcja jest dostępna w przypadku protokołów NEAR i

© Acronis International GmbH, 2003-2024

Opcja uwierzytelniania	Opis
	Udostępnianie ekranu firmy Apple. Z tej możliwości można skorzystać w celu uwierzytelnienia na potrzeby pomocy zdalnej.
Poproś o zgodę na sterowanie	Połączenie zdalne będzie można nawiązać w trybie sterowania po uzyskaniu zezwolenia od użytkownika zalogowanego na obciążeniu zdalnym. Ta opcja jest dostępna w przypadku protokołów NEAR i Udostępnianie ekranu firmy Apple. Z tej możliwości można skorzystać w celu uwierzytelnienia na potrzeby pomocy zdalnej.

8. Kliknij **Połącz**, a następnie kliknij sesję, która ma zostać wyświetlona (jeśli na obciążeniu jest dostępna więcej niż jedna sesja użytkownika).

   Program Klient rozwiązania Connect otworzy nowe okno podglądu, w którym będzie widoczny pulpit obciążenia zdalnego. Podgląd zawiera pasek narzędzi z dodatkowymi czynnościami, które można wykonać na obciążeniu zdalnym po nawiązaniu połączenia zdalnego. Aby uzyskać więcej informacji, zobacz "Korzystanie z paska narzędzi w oknie podglądu" (s. 1113).

Nawiązywanie połączenia z obciążeniem zarządzanym przy użyciu klienta internetowego

Istnieje możliwość nawiązania połączenia pulpitu zdalnego z obciążeniem zarządzanym przy użyciu klienta internetowego.

Wymagania wstępne

- Obciążenie ma przypisane standardowy limit usługi.
- Do obciążenia zarządzanego zastosowano plan zarządzania zdalnego z włączonym protokołem RDP.
- Na obciążeniu zarządzanym włączono protokół RDP.
- Przeglądarka obsługuje język HTML5.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.

Aby nawiązać połączenie zdalne z obciążeniem przy użyciu klienta internetowego

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie, z którym chcesz się połączyć zdalnie, a następnie kliknij **Pulpit zdalny** > **Połącz przez klienta internetowego**.
3. Wprowadź nazwę logowania i hasło w celu uzyskania dostępu do obciążenia, a następnie kliknij **Połącz**.

© Acronis International GmbH, 2003-2024

Uwaga
Jeśli do obciążenia zostały przypisane poświadczenia, uwierzytelnianie zostanie przeprowadzone automatycznie i ten krok zostanie pominięty. Aby uzyskać więcej informacji, zobacz "Przypisywanie poświadczeń do obciążenia" (s. 1099).

Przesyłanie plików

Możesz łatwo przesyłać pliki między obciążeniem lokalnym a obciążeniem zarządzanym.

Wymagania wstępne

- Do obciążenia zastosowano plan zarządzania zdalnego z włączonym protokołem NEAR i funkcją Przesyłanie plików.
- Do obciążenia zastosowano limit Zarządzanie zaawansowane.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.

Aby zdalnie przesyłać pliki między swoim obciążeniem a obciążeniem zarządzanym

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Kliknij obciążenie, które ma uczestniczyć w przesyłaniu plików.
3. Kliknij **Zarządzaj**, a następnie **Prześlij pliki**.
4. W zależności od tego, czy na obciążeniu jest zainstalowany program Klient rozwiązania Connect, wykonaj jedną z następujących czynności:
   - Jeśli program Klient rozwiązania Connect nie jest zainstalowany, pobierz go, zainstaluj, a następnie w wyświetlonym wyskakującym okienku z monitem o potwierdzenie kliknij **Pozwól**.
   - Jeśli program Klient rozwiązania Connect jest już zainstalowany, w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Otwórz klienta rozwiązania Connect**.
5. W oknie **Uwierzytelnianie** wybierz opcję uwierzytelniania, a następnie wpisz wymagane poświadczenia.

Opcja uwierzytelniania	Opis
Przy użyciu poświadczeń dostępu do obciążenia zdalnego	Połączenie zdalne będzie można nawiązać po podaniu nazwy użytkownika i hasła administratora na obciążeniu zdalnym.
Poproś o zezwolenie na przesyłanie plików	Pliki będzie można przesyłać po uzyskaniu zezwolenia od użytkownika zalogowanego na obciążeniu zdalnym.

6. W oknie **Przesyłanie plików** przejrzyj pliki i przeciągnij je do odpowiedniej lokalizacji docelowej.

© Acronis International GmbH, 2003-2024

Uwaga
Pliki z obciążenia lokalnego są widoczne w lewym okienku, a pliki z obciążenia zdalnego są widoczne w prawym okienku.
Po rozpoczęciu przesyłania plików operacja ta zostanie uwzględniona na liście w okienku **Zadania**.

7. [Opcjonalnie] Jeśli zechcesz usunąć ukończone zadania z okienka **Zadania**, kliknij **Wyczyść zakończone**.
8. Gdy już wszystkie operacje przesyłania zostaną ukończone, zamknij okno.

Wykonywanie czynności związanych ze sterowaniem na obciążeniach zarządzanych

Możesz zarządzać obciążeniem zdalnym, wykonując na nim podstawowe czynności związane ze sterowaniem: opróżnienie kosza, uśpienie, uruchom ponownie, zamknięcie systemu i wyloguj użytkownika zdalnego.

Wymagania wstępne

- Do obciążenia zastosowano standardowy limit usługi.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.

Opróżnij kosz

Aby opróżnić kosz na obciążeniu zdalnym

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Kliknij obciążenie, na którym chcesz wykonać tę czynność.
3. Kliknij **Zarządzaj**, a następnie **Opróżnij kosz**.
4. Wybierz sesję użytkownika, w ramach której chcesz wykonać tę czynność, a następnie kliknij **Opróżnij kosz**.

Uśpij

Aby uśpić obciążenie zdalne

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Kliknij obciążenie, na którym chcesz wykonać tę czynność.
3. Kliknij **Zarządzaj**, a następnie **Uśpij**.

Uruchom ponownie

Aby ponownie uruchomić obciążenie zdalne

© Acronis International GmbH, 2003-2024

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Kliknij obciążenie, na którym chcesz wykonać tę czynność.
3. Kliknij **Zarządzaj**, a następnie **Uruchom ponownie**.
   - W przypadku obciążenia z systemem Windows określ, czy użytkownik, który jest aktualnie lokalnie zalogowany na obciążeniu, ma mieć możliwość zapisania zmian przed ponownym uruchomieniem obciążenia, zaznacz tego użytkownika, a następnie kliknij **Uruchom ponownie**.
   - W przypadku obciążenia z systemem macOS określ, czy użytkownik, który jest aktualnie lokalnie zalogowany na obciążeniu, ma mieć możliwość zapisania zmian przed ponownym uruchomieniem obciążenia, a następnie kliknij **Uruchom ponownie**.
   - W przypadku obciążenia z systemem Linux kliknij **Uruchom ponownie**.

Zamknij system

Aby zamknąć system obciążenia zdalnego

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Kliknij obciążenie, na którym chcesz wykonać tę czynność.
3. Kliknij **Zarządzaj**, a następnie **Zamknij system**.
   - W przypadku obciążenia z systemem Windows określ, czy użytkownik, który jest aktualnie lokalnie zalogowany na obciążeniu, ma mieć możliwość zapisania zmian przed zamknięciem systemu obciążenia, zaznacz tego użytkownika, a następnie kliknij **Zamknij system**.
   - W przypadku obciążenia z systemem macOS określ, czy użytkownik, który jest aktualnie lokalnie zalogowany na obciążeniu, ma mieć możliwość zapisania zmian przed zamknięciem systemu obciążenia, a następnie kliknij **Zamknij system**.
   - W przypadku obciążenia z systemem Linux kliknij **Zamknij system**.

Wyloguj użytkownika zdalnego

Aby wylogować użytkownika na obciążeniu zdalnym

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Kliknij obciążenie, na którym chcesz wykonać tę czynność.
3. Kliknij **Zarządzaj**, a następnie **Wyloguj użytkownika zdalnego**.
4. Zaznacz użytkownika, którego chcesz wylogować, a następnie kliknij **Wyloguj**.

Monitorowanie obciążeń przy użyciu funkcji przesyłania zrzutów ekranu

Istnieje możliwość monitorowania statusu obciążenia dzięki funkcji przesyłania zrzutów ekranu.

© Acronis International GmbH, 2003-2024

Wymagania wstępne

- Na obciążeniu zostaje zastosowany plan zarządzania zdalnego z włączoną funkcją przesyłania zrzutów ekranu.
- Agent ochrony ma aktualną wersję i obsługuje funkcję przesyłania zrzutów ekranu.
- Do obciążenia jest zastosowany limit usługi Zarządzanie zaawansowane.
- Obciążenie jest w trybie online.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.

Monitorowanie obciążenia przy użyciu funkcji przesyłania zrzutów ekranu

Aby monitorować obciążenie przy użyciu funkcji przesyłania zrzutów ekranu

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Przesyłanie zrzutu ekranu**.
2. Kliknij obciążenie, które chcesz monitorować.
3. Wybierz sesję użytkownika.
4. Wybierz wyświetlacz.
5. Wybierz częstotliwość odświeżania, czyli odstępy, w jakich ma być wykonywany nowy zrzut ekranu pulpitu.
6. Wybierz jakość obrazu.
7. Aby pobrać zrzut ekranu, kliknij ikonę pobierania.

Wykonywanie zrzutu ekranu obciążenia

Aby wykonać zrzut ekranu obciążenia zarządzanego

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Komputery z agentami**.
2. Kliknij obciążenie, z którego chcesz wykonać zrzut ekranu.
3. Kliknij **Zarządzaj**, a następnie kliknij **Zrób zrzut ekranu pulpitu**.
   Zostanie otwarty ekran **Przesyłanie zrzutu ekranu** z już zaznaczonym odpowiednim obciążeniem. W zależności od ustawień planu zarządzania zdalnego zastosowanego na obciążeniu zrzut ekranu pojawi się teraz lub po zatwierdzeniu prośby przez użytkownika obciążenia zdalnego.

Obserwowanie wielu obciążeń zarządzanych naraz

W jednym oknie można obserwować pulpity wielu obciążeń zdalnych naraz.

Uwaga
Liczba pulpitów, które mogą być widoczne w tym oknie, zależy od wielkości monitora.

© Acronis International GmbH, 2003-2024

Wymagania wstępne

- W planach zarządzania zdalnego stosowanych do tych obciążeń jest włączony protokół NEAR lub protokół Udostępnianie ekranu firmy Apple.
- Do obciążenia jest zastosowany limit usługi Zarządzanie zaawansowane.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.

Aby obserwować wiele obciążeń naraz

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz obciążenia, które chcesz obserwować.
3. Kliknij **Multiwidok**.
4. W zależności od tego, czy na obciążeniu jest zainstalowany program Klient rozwiązania Connect, wykonaj jedną z następujących czynności:
   - Jeśli program Klient rozwiązania Connect nie jest zainstalowany, pobierz go, zainstaluj, a następnie w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Pozwól**.
   - Jeśli program Klient rozwiązania Connect jest już zainstalowany, w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Otwórz klienta rozwiązania Connect**.
5. W oknie **Uwierzytelnianie** wybierz opcję uwierzytelniania, a następnie wpisz wymagane poświadczenia.

Opcja uwierzytelniania	Opis
Przy użyciu poświadczeń dostępu do obciążenia zdalnego	Połączenie zdalne będzie można nawiązać po podaniu nazwy użytkownika i hasła administratora na obciążeniu zdalnym.
Poproś o zgodę na obserwację	Połączenie zdalne będzie można nawiązać w trybie obserwacji po uzyskaniu zezwolenia od użytkownika zalogowanego na obciążeniu zdalnym.

6. Jeśli chcesz używać tej samej metody uwierzytelniania i poświadczeń przy nawiązywaniu połączenia ze wszystkimi obciążeniami zdalnymi, które zostały wybrane w kroku 2, wybierz **Użyj w przypadku innych komputerów**.
7. Kliknij **Połącz**.

   Na pasku narzędzi okna z multiwidokiem możesz wybrać tryb widoku, w którym chcesz nawiązać połączenie z obciążeniem. Spowoduje to otwarcie osobnego okna z podglądem tego obciążenia.

© Acronis International GmbH, 2003-2024

Uwaga
Jeśli któreś z wybranych obciążeń jest offline lub ma zainstalowanego agenta w nieaktualnej wersji, nie będzie widoczne w oknie multiwidoku.
Wszystkie połączenia z obciążeniami zdalnymi w multiwidoku są w trybie **Tylko do przeglądania**.

Praca z obciążeniami niezarządzanymi

Obciążenia niezarządzane to obciążenia, na których nie ma zainstalowanego agenta Ochrona.

Na niezarządzanych obciążeniach zdalnych można wykonywać następujące czynności:

- Nawiązywanie połączeń na potrzeby pomocy zdalnej przy użyciu aplikacji Acronis Quick Assist
- Nawiązywanie połączeń na potrzeby pulpitu zdalnego lub pomocy zdalnej przy użyciu adresu IP
- Przesyłanie plików między własnym obciążeniem a obciążeniem zdalnym przy użyciu aplikacji Quick Assist

Uwaga
Aby nawiązać połączenie zdalne z obciążeniem niezarządzanym przy użyciu aplikacji Quick Assist, dopilnuj, by zostały spełnione następujące warunki:

- Dla dzierżawcy-klienta aktywowano pakiet Zarządzanie zaawansowane.
- Aplikacja Quick Assist jest uruchomiona na obciążeniu zdalnym, z którym chcesz nawiązać połączenie.

Nawiązywanie połączeń z obciążeniami niezarządzanymi przy użyciu aplikacji Acronis Quick Assist

Za pomocą aplikacji Quick Assist możesz na żądanie ustanowić połączenie zdalne z obciążeniem niezarządzanym i jednorazowo udzielić pomocy.

Wymagania wstępne

- Do dzierżawcy-klienta przypisano pakiet Zarządzanie zaawansowane.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.
- Użytkownik zdalny podał identyfikator obciążenia i kod dostępu z aplikacji Quick Assist.
- Użytkownik zdalny pobrał i uruchomił aplikację Acronis Quick Assist.

Aby nawiązać połączenie z obciążeniem na potrzeby pomocy zdalnej przy użyciu aplikacji Quick Assist

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij **Quick Assist**.

© Acronis International GmbH, 2003-2024

3. W oknie **Quick Assist** wprowadź identyfikator obciążenia podany przez użytkownika, a następnie wybierz **Połącz**.
4. Kliknij **Połącz**.
5. W zależności od tego, czy na obciążeniu jest zainstalowany program Klient rozwiązania Connect, wykonaj jedną z następujących czynności:
   - Jeśli program Klient rozwiązania Connect nie jest zainstalowany, pobierz go, zainstaluj, a następnie w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Pozwól**.
   - Jeśli program Klient rozwiązania Connect jest już zainstalowany, w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Otwórz klienta rozwiązania Connect**.
6. W oknie **Uwierzytelnianie** wprowadź kod dostępu.
7. Program Klient rozwiązania Connect otworzy nowe okno podglądu, w którym będzie widoczny pulpit obciążenia zdalnego. Podgląd zawiera pasek narzędzi z dodatkowymi czynnościami, które można wykonać na obciążeniu zdalnym po nawiązaniu połączenia zdalnego. Aby uzyskać więcej informacji, zobacz "Korzystanie z paska narzędzi w oknie podglądu" (s. 1113).

Nawiązywanie połączeń z obciążeniami niezarządzanymi przy użyciu adresów IP

Jeśli obciążenie niezarządzane znajduje się w tej samej sieci LAN, można nawiązać z nim połączenie przy użyciu jego adresu IP na potrzeby zdalnego sterowania lub pomocy zdalnej. Takie połączenie nie wymaga dostępu do Internetu.

Wymagania wstępne

- Do dzierżawcy-klienta przypisano pakiet Zarządzanie zaawansowane.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.

Aby nawiązać połączenie z obciążeniem na potrzeby pulpitu zdalnego lub pomocy zdalnej przy użyciu adresu IP

1. W konsoli Cyber Protect przejdź do sekcji **Wszystkie urządzenia**.
2. Kliknij **Quick Assist**.
3. Kliknij kartę **Za pomocą adresu IP**.
4. Wprowadź adres IP i port obciążenia.
5. W zależności od systemu operacyjnego obciążenia zdalnego wybierz protokół połączenia: RDP (w przypadku obciążeń z systemem Windows) lub Udostępnianie ekranu firmy Apple (w przypadku obciążeń z systemem macOS).

© Acronis International GmbH, 2003-2024

Uwaga
Połączenia przez protokół RDP obsługują czynność pulpitu zdalnego, a połączenia przez Udostępnianie ekranu firmy Apple obsługują czynności zarówno pulpitu zdalnego, jak i pomocy zdalnej.

6. Kliknij **Połącz**.
7. W oknie **Uwierzytelnianie** wpisz wymagane poświadczenia.

W przypadku połączeń nawiązanych przy użyciu protokołu Udostępnianie ekranu firmy Apple program Klient rozwiązania Connect otworzy nowe okno podglądu, w którym będzie widoczny pulpit obciążenia zdalnego. Podgląd zawiera pasek narzędzi z dodatkowymi czynnościami, które można wykonać na obciążeniu zdalnym po nawiązaniu połączenia zdalnego. Aby uzyskać więcej informacji, zobacz "Korzystanie z paska narzędzi w oknie podglądu" (s. 1113).

Przesyłanie plików za pośrednictwem aplikacji Acronis Quick Assist

Za pomocą aplikacji Quick Assist można przesyłać pliki między swoim obciążeniem a obciążeniami niezarządzanymi.

Wymagania wstępne

- Do dzierżawcy-klienta przypisano pakiet Zarządzanie zaawansowane.
- Dla Twojego konta użytkownika w rozwiązaniu Acronis Cyber Protect Cloud zostało włączone uwierzytelnianie dwuskładnikowe.
- Użytkownik zdalny pobrał i uruchomił aplikację Acronis Quick Assist.
- Użytkownik zdalny podał identyfikator komputera i kod dostępu z aplikacji Quick Assist.

Aby przesyłać pliki z obciążenia przy użyciu aplikacji Quick Assist

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij **Quick Assist**.
3. W oknie **Quick Assist** wprowadź identyfikator obciążenia podany przez użytkownika, a następnie wybierz **Przesyłanie plików**.
4. Kliknij **Połącz**.
5. W zależności od tego, czy na obciążeniu jest zainstalowany program Klient rozwiązania Connect, wykonaj jedną z następujących czynności:
   - Jeśli program Klient rozwiązania Connect nie jest zainstalowany, pobierz go, zainstaluj, a następnie w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Pozwól**.
   - Jeśli program Klient rozwiązania Connect jest już zainstalowany, w wyświetlonym wyskakującym okienku z monitem o potwierdzenie wybierz **Otwórz klienta rozwiązania Connect**.

© Acronis International GmbH, 2003-2024

6. W oknie **Uwierzytelnianie** wprowadź kod dostępu.
7. W oknie **Przesyłanie plików** przejrzyj pliki i przeciągnij je do odpowiedniej lokalizacji docelowej.

   Uwaga
   Pliki z obciążenia lokalnego są widoczne w lewym okienku, a pliki z obciążenia zdalnego są widoczne w prawym okienku.
   Po rozpoczęciu przesyłania plików operacja ta zostanie uwzględniona na liście w okienku **Zadania**.

8. [Opcjonalnie] Jeśli zechcesz usunąć ukończone zadania z okienka **Zadania**, kliknij **Wyczyść zakończone**.
9. Gdy już wszystkie operacje przesyłania zostaną ukończone, zamknij okno.

Korzystanie z paska narzędzi w oknie podglądu

Po nawiązaniu połączenia z obciążeniem zdalnym możesz korzystać z paska narzędzi w oknie podglądu, aby szybko wykonywać różne czynności.

Ikona	Opis
	Rzeczywisty rozmiar Umożliwia skalowanie pulpitu obciążenia zdalnego tak, aby jeden piksel pulpitu zdalnego odpowiadał jednemu pikselowi w oknie podglądu.
	Dopasuj do okna Umożliwia skalowanie pulpitu obciążenia zdalnego w celu dopasowania go do okna podglądu.
	Zablokuj i **Odblokuj ekran** Powoduje wyświetlanie widoku zastępczego na ekranie obciążenia zdalnego, aby użytkownik zdalny nie widział, co robisz.
	Zrób zrzut ekranu Zapisz obrazu pulpitu serwera zdalnego w pliku lokalnym.
	Wybierz wyświetlacz Wybierz wyświetlacz obciążenia zdalnego, który chcesz zobaczyć, i odpowiadającą Ci rozdzielczość. Opcja dostępna w przypadku połączeń z systemem macOS przy użyciu protokołu Udostępnianie ekranu firmy Apple oraz połączeń z dowolnym systemem operacyjnym przy użyciu protokołu NEAR.
	Jakość obrazu

© Acronis International GmbH, 2003-2024

Ikona	Opis
	Umożliwia dostosowywanie jakości obrazu ekranu zdalnego — od czarno-białego do najwyższej możliwej jakości — w przypadku połączeń przy użyciu protokołu Udostępnianie ekranu firmy Apple.
	Jakość obrazu w ramach połączeń przy użyciu protokołu NEAR Umożliwia regulowanie stosunku jakości do wydajności w przypadku połączeń nawiązanych przy użyciu protokołu NEAR. Lewa strona suwaka (obraz Płynny) oznacza pierwszeństwo wydajności nad jakością obrazu, prawa strona (obraz Ostry) oznacza najlepszą jakość obrazu z ekranu pulpitu zdalnego, ale prawdopodobnie gorszą wydajność.
	Wyślij Ctrl+Alt+Del Powoduje wysłanie do obciążenia zdalnego sekwencji naciśnięć klawiszy Ctrl + Alt + Delete. Opcja dostępna w przypadku obciążeń z systemami Windows i Linux.
	Przesyłanie plików Umożliwia otwarcie okna Menedżer plików w celu wymiany plików między obciążeniem zdalnym i lokalnym. Opcja dostępna w przypadku połączeń przy użyciu protokołu NEAR.
	Przypnij pasek narzędzi Powoduje wyłączenie automatycznego ukrywania paska narzędzi w oknie podglądu. Opcja dostępna w przypadku obciążeń z systemem Windows.
	Pełny ekran Umożliwia przełączenie na tryb pełnoekranowy i przeskalowanie obciążenia zdalnego tak, aby całkowicie wypełnić ekran lokalny. Opcja dostępna w przypadku obciążeń z systemem Windows.
	Zamknij Powoduje zamknięcie okna podglądu i zakończenie sesji zdalnego sterowania. Opcja dostępna w przypadku obciążeń z systemem Windows.

W zależności od typu połączenia po kliknięciu ikony **Inne** mogą być dostępne dodatkowe opcje.

Opcja	Opis
Rozpocznij nagrywanie / Zatrzymaj nagrywanie	Umożliwia nagrywanie bieżącej sesji pulpitu zdalnego. Nagrania sesji są zapisywane jako pliki .crec na

© Acronis International GmbH, 2003-2024

Opcja	Opis
	maszynie lokalnej. Pliki .crec można otwierać za pomocą narzędzia Acronis Klient rozwiązania Connect. Opcja dostępna w przypadku połączeń przy użyciu protokołu NEAR.
Automatyczna synchronizacja schowka	W przypadku włączenia tej opcji klient będzie automatycznie synchronizować lokalny schowek ze schowkiem komputera zdalnego. Opcja dostępna w przypadku połączeń przy użyciu protokołów NEAR i Udostępnianie ekranu firmy Apple
Wyślij zawartość schowka **Pobierz zawartość schowka**	Włączenie opcji **Wyślij zawartość schowka** powoduje zastąpienie zawartości schowka komputera zdalnego zawartością schowka lokalnego. Włączenie opcji **Pobierz zawartość schowka** powoduje przesłanie zawartości schowka komputera zdalnego do schowka lokalnego.
Klawiatura inteligentna / Surowe naciśnięcia klawiszy / Surowe naciśnięcia klawiszy ze wszystkimi skrótami	Umożliwia zmienienie trybu wprowadzania danych z klawiatury w ramach bieżącego połączenia. **Klawiatura inteligentna** — klient przesyła do komputera zdalnego kody Unicode lokalnie wpisywanych symboli. **Surowe naciśnięcia klawiszy** — klient używa surowych kodów naciskanych klawiszy klawiatury. **Surowe naciśnięcia klawiszy ze wszystkimi skrótami** — klient wyłącza lokalne skróty systemowe, aby one również były przesyłane do zdalnego systemu operacyjnego.
Fokus klawiatury po wskazaniu myszą	W przypadku włączenia tej opcji klient przechwytuje dane z klawiatury tylko wtedy, gdy lokalny kursor myszy znajduje się na oknie podglądu. Gdy ta opcja jest wyłączona, klient przechwytuje naciśnięcia klawiszy, gdy jego okno jest aktywne.
Pokaż informacje o połączeniu / Ukryj informacje o połączeniu	W przypadku zaznaczenia opcji **Pokaż informacje o połączeniu** nad ekranem pulpitu zdalnego pojawi się mały panel z najważniejszymi informacjami o bieżącym połączeniu.
Dźwięk zdalny	Umożliwia klientowi przekierowanie dźwięku z komputera zdalnego na lokalny. Opcja dostępna w przypadku połączeń przy użyciu

© Acronis International GmbH, 2003-2024

Opcja	Opis
	protokołu NEAR.
Preferencje	Skonfiguruj ustawienia programu Klient rozwiązania Connect. Aby uzyskać więcej informacji, zobacz "Konfigurowanie ustawień programu Klient rozwiązania Connect" (s. 1117).

Nagrywanie i odtwarzanie sesji zdalnych

Sesję zdalną można nagrać przy użyciu protokołu NEAR w narzędziu Acronis Klient rozwiązania Connect.

Aby nagrać sesję zdalną

1. Na pasku narzędzi w ognie podglądu w narzędziu Klient rozwiązania Connect kliknij **Inne** i wybierz **Rozpocznij nagrywanie**.
2. Wybierz nazwę i lokalizację nagrania.

   Domyślnie plik będzie mieć nazwę złożoną z bieżącej daty i godziny oraz będzie zlokalizowany w folderze **Dokumenty** w katalogu głównym bieżącego użytkownika. Gdy nagrywanie jest aktywne, na pasku narzędzi okna **podglądu** zobaczysz migające czerwone kółko nad prawym górnym rogiem ekranu połączenia zdalnego i czasomierz nagrywania.
3. Aby zatrzymać nagrywanie, kliknij **Inne**, a następnie kliknij **Zatrzymaj nagrywanie**. Na komputerze Mac możesz też kliknąć **Stop** na pasku narzędzi.

   Wszystkie pliki .crec utworzone przez narzędzie Acronis Klient rozwiązania Connect będą domyślnie otwierane za pomocą narzędzia Acronis Klient rozwiązania Connect.

Aby odtworzyć nagranie

1. Znajdź plik nagrania.
2. Otwórz go.

   Zostanie otwarty odtwarzacz narzędzia Acronis Klient rozwiązania Connect. Należy pamiętać, że nie ma możliwości poruszania się po nagraniu. Aby znaleźć określony moment w nagraniu, trzeba poczekać, aż odtwarzacz do niego dotrze.
3. [Opcjonalnie] Aby dostosować prędkość odtwarzania, użyj ikon **<<** i **>>** w sekcji sterowania odtwarzaniem.

   Nagranie jest przechowywane jako sekwencja zdarzeń, które zostały przesłane do i z serwera zdalnego podczas połączenia. Zapewnia to najlepszą jakość nagrania przy minimalnym rozmiarze pliku. Oznacza to jednak również, że nie ma możliwości poruszania się po nagraniu. Obecnie nie ma także możliwości konwersji nagrań na format wideo.

© Acronis International GmbH, 2003-2024

Konfigurowanie ustawień programu Klient rozwiązania Connect

Po zainstalowaniu na obciążeniu programu Klient rozwiązania Connect możesz skonfigurować jego ustawienia zgodnie z własnymi preferencjami.

Aby skonfigurować ustawienia programu Klient rozwiązania Connect

1. W menu startowym znajdź program **Klient rozwiązania Connect** i go uruchom.
2. Skonfiguruj ustawienia dostępne na karcie **Ogólne**.

Opcja	Opis
Zapisz dzienniki w wersji pełnej	Zaznacz tę opcję, aby zezwolić programowi Klient rozwiązania Connect na zapisywanie dzienników w wersji pełnej. Jeśli ta opcja będzie wyłączona, klient zapisze w pliku dziennika tylko ogólne informacje.
Ustawienia serwera proxy	Wybierz, czy chcesz użyć domyślnego systemowego serwera proxy, czy skonfigurować niestandardowy serwer proxy SOCKSS.

3. Skonfiguruj ustawienia dostępne na karcie **Podgląd**.

Opcja	Opis
Proś o potwierdzenie przy zamykaniu podglądu	Zaznacz tę opcję, jeśli chcesz, aby program Klient rozwiązania Connect wyświetlał monit o potwierdzenie przy próbie zamknięcia okna podglądu w celu zapobieżenia przypadkowemu zamknięciu.
Przy zminimalizowanym oknie	Zaznacz tę opcję, aby aktywność podglądu była zawieszana po zminimalizowaniu jego okna — w celu zmniejszenia obciążenia procesora.
Przy zmaksymalizowanym oknie	Zaznacz tę opcję, aby po zmaksymalizowaniu okna był włączany tryb pełnoekranowy.
Przenoszenie przy użyciu schowka	Włącz wyświetlanie w oknie podglądu wskaźnika przenoszenia danych przy użyciu schowka, gdy skopiujesz bądź wkleisz tekst lub obrazy.
Tryb klawiatury	Włącz wyświetlanie na pasku tytułu okna podglądu wskaźnika trybu wprowadzania, gdy zdarzenia myszy i klawiatury są wysyłane do komputera zdalnego.
Schowek	Zaznacz **Automatycznie synchronizuj schowek**, aby włączyć automatyczną synchronizację schowka, jeśli taka funkcja jest dostępna.

© Acronis International GmbH, 2003-2024

Opcja	Opis
Wysyłaj zdarzenia klawiatury	Określ, czy dane wprowadzane za pomocą lokalnej klawiatury mają być przechwytywane zawsze, gdy jest aktywne okno programu Klient rozwiązania Connect, czy tylko wtedy, gdy zatrzymano na nim wskaźnik lokalnej myszy.
Kolor tła podglądu	Zmiana koloru tła okna podglądu.
Automatycznie połącz ponownie	Zaznacz **Włącz automatyczne ponowne połączenie**, jeśli chcesz, aby program Klient rozwiązania Connect automatycznie wznawiał zerwane połączenie.
H.264	Możesz wyłączyć dekodery sprzętowe.
Zamknij w stanie bezczynności	Wybierz czas bezczynności, po którym okno podglądu ma zostać zamknięte.

4. Skonfiguruj ustawienia dostępne na karcie **Klawiatura**.

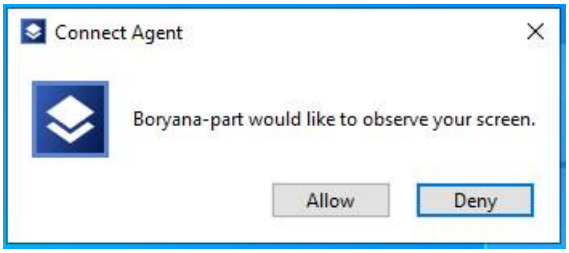
Opcja	Opis
Mapowania modyfikatorów	Zmień działanie klawiszy modyfikujących za pomocą menu podręcznego. Ustawienia te są zapisywane osobno dla każdego protokołu połączeń: NEAR, Udostępnianie ekranu firmy Apple i RDP.
Tryb wprowadzania	W przypadku każdego typu połączenia (wybranego w nagłówku okienka) wybierz domyślny tryb wprowadzania danych za pomocą klawiatury.

5. Kliknij **OK**.

Powiadomienia dotyczące pulpitu zdalnego

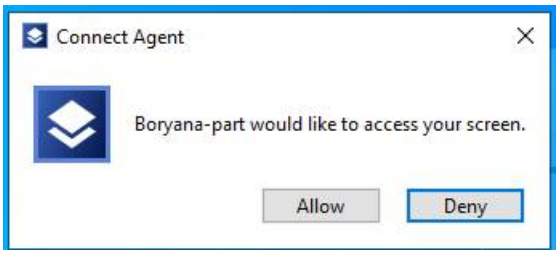
Moduł Agent rozwiązania Connect inicjuje wyświetlanie okien dialogowych z informacjami (powiadomieniami) o czynnościach na pulpicie obciążenia zdalnego w następujących przypadkach:

- Gdy próbujesz nawiązać połączenie zdalne z obciążeniem, wysyłając prośbę o zgodę na obserwację. Użytkownik zalogowany na obciążeniu zdalnym może wyrazić zgodę lub jej odmówić.

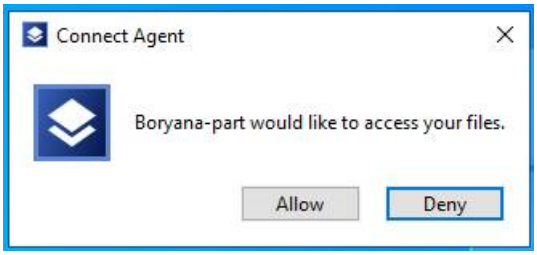


- Gdy próbujesz nawiązać połączenie zdalne z obciążeniem, wysyłając prośbę o zgodę na sterowanie. Użytkownik zalogowany na obciążeniu zdalnym może wyrazić zgodę lub jej odmówić.

© Acronis International GmbH, 2003-2024



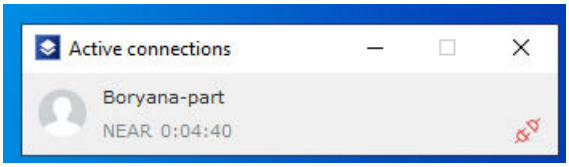
- Gdy próbujesz dokonać wymiany plików między swoim obciążeniem a obciążeniem zdalnym, wysyłając prośbę o zgodę na przesłanie plików. Użytkownik zalogowany na obciążeniu zdalnym może wyrazić zgodę lub jej odmówić.



Po ustanowieniu połączenia pulpitu zdalnego z obciążeniem użytkownik zalogowany na obciążeniu zobaczy inne powiadomienie o połączeniu, które zawiera następujące informacje:

- Nazwa użytkownika, który nawiązał połączenie zdalne
- Protokół użyty do nawiązania połączenia zdalnego
- Czas trwania połączenia zdalnego

Użytkownik zalogowany lokalnie na obciążeniu zdalnym może w każdej chwili zakończyć połączenie, klikając ikonę **Rozłącz** lub ikonę **Zamknij**.



© Acronis International GmbH, 2003-2024

Monitorowanie kondycji i wydajności obciążeń

Możesz monitorować parametry systemu i kondycję obciążeń organizacji. Jeśli parametr odbiega od normy, niezwłocznie otrzymasz stosowne powiadomienie, co pozwoli szybko rozwiązać wykryty problem. Możesz też skonfigurować niestandardowe alerty i automatyczne czynności w ramach reagowania. Są to czynności, które będą wykonywane automatycznie w celu wyeliminowania anomalii w zachowaniu obciążenia.

Uwaga
Funkcja monitorowania wymaga zainstalowania na obciążeniach agenta Ochrona w wersji 15.0.35324 lub nowszej.

Plany monitorowania

Aby rozpocząć monitorowanie parametrów dotyczących wydajności, sprzętu, oprogramowania, systemu i zabezpieczeń zarządzanych obciążeń, należy zastosować do nich plan monitorowania. Plany monitorowania składają się z różnych monitorów, które można włączać i konfigurować. Niektóre monitory obsługują monitorowanie oparte na wykrywaniu anomalii. Dodatkowe informacje na temat planów monitorowania można znaleźć w sekcji "Plany monitorowania" (s. 1156). Dodatkowe informacje na temat dostępnych monitorów, które można konfigurować w planach monitorowania, można znaleźć w sekcji "Konfigurowalne monitory" (s. 1121).

Jeśli agentowi z jakiegoś powodu nie uda się zebrać danych z obciążenia, system wygeneruje alert.

Typy monitorowania

Należy skonfigurować typ monitorowania dla każdego monitora włączonego w planie. Typ monitorowania określa algorytm, którego monitor będzie używać do oszacowania normalnego zachowania i odchyleń obciążenia. Występują dwa typy monitorowania: Wykrywanie progów i Wykrywanie anomalii. Niektóre monitory obsługują tylko monitorowanie typu Wykrywanie progów.

Monitorowanie typu Wykrywanie progów polega na obserwowaniu, czy wartości parametrów są powyżej lub poniżej skonfigurowanej wartości progu. W przypadku tego typu monitorowania to użytkownik odpowiada za zdefiniowanie poprawnych wartości progów dla obciążeń. System ustala normalność zachowania na podstawie tych statycznych wartości progów — bez uwzględnienia innych szczególnych warunków, które mogą powodować takie zachowanie. Dlatego monitorowanie typu Wykrywanie progów może być mniej dokładne w porównaniu z monitorowaniem typu Wykrywanie anomalii.

W przypadku monitorowania typu Wykrywanie anomalii wykorzystywane jest uczenie maszynowe do tworzenia wzorców normalnych zachowań danego obciążenia i wykrywania zachowań odbiegających od normy. Aby uzyskać więcej informacji, zobacz "Monitorowanie typu Wykrywanie anomalii" (s. 1121).

© Acronis International GmbH, 2003-2024

Monitorowanie typu Wykrywanie anomalii

W przypadku monitorowania typu Wykrywanie anomalii używane są modele uczenia maszynowego w celu utworzenia wzorców normalnych zachowań dla danego obciążenia oraz wykrywania anomalii (nieoczekiwanych wzrostów danych w seriach czasowych) w zachowaniu obciążenia. Po aktywowaniu tego typu monitorowania system tworzy model i rozpoczyna proces szkolenia oraz koryguje model dla konkretnego obciążenia na podstawie danych zbieranych z tego obciążenia. Oznacza to, że na początku okresu szkolenia dane mogą nie być zupełnie dokładne. Utworzenie rzetelnego modelu wymaga co najmniej trzech tygodni szkolenia modelu. W miarę jak system gromadzi więcej danych i analizuje zestawy danych historycznych, stopniowo udoskonala model i tworzy dynamiczne górne i dolne progi dla każdego wskaźnika obciążenia. Ten typ monitorowania jest bardziej elastyczny w porównaniu z monitorowaniem z wykrywaniem progów, ponieważ system monitoruje wartości parametrów i ich kontekst. Na przykład, określone obciążenie może być większe w pewnych godzinach dnia i jest to sytuacja normalna. W przypadku monitorowania z wykrywaniem progów nastąpiłoby błędne zinterpretowanie takiej sytuacji jako zachowania odbiegającego od normy i wywołany zostałby alert.

Możesz zresetować modele uczenia maszynowego obciążenia. W takim przypadku system usunie wszystkie dane i modele dla monitorów zastosowanych do obciążenia. Aby uzyskać więcej informacji, zobacz "Resetowanie modeli uczenia maszynowego" (s. 1167).

Platformy obsługiwane w ramach monitorowania

Funkcja monitorowania jest obsługiwana w przypadku następujących systemów operacyjnych.

Obsługiwane wersje systemu Windows	Obsługiwane wersje systemu macOS
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura)

Konfigurowalne monitory

Funkcja monitorowania obsługuje następujące monitory, które podzielono na sześć kategorii: Sprzęt, Wydajność, Oprogramowanie, System, Zabezpieczenia oraz Niestandardowe.

© Acronis International GmbH, 2003-2024

Monitoruj	Opis	Obsługiwane systemy operacyjne	Częstotliwość zbierania danych	Obsługa monitorowania typu Wykrywanie anomalii	Dostępność w ramach ochrony typu Standardowy lub pakiecie Zarządzanie zaawansowane
Sprzęt					
Miejsce na dysku	Monitoruje ilość wolnego miejsca na określonym dysku obciążenia.	Windows macOS	1 min	Tak	Ochrona standardowa
Temperatura procesora	Monitoruje temperaturę procesora.	Windows macOS	30 s	Tak	Zarządzanie zaawansowane
Temperatura procesora graficznego	Monitoruje temperaturę procesora graficznego.	Windows macOS	30 s	Tak	Zarządzanie zaawansowane
Zmiany sprzętowe	Monitoruje zmiany sprzętowe, takie jak dodanie, usunięcie lub wymiana sprzętu w obciążeniu	Windows macOS	24 godz.	Nie	Ochrona standardowa
Wydajność					
Użycie procesora	Monitoruje ogólny poziom użycia procesora (według wszystkich procesorów w obciążeniu).	Windows macOS	30 s	Tak	Zarządzanie zaawansowane

© Acronis International GmbH, 2003-2024

Monitoruj	Opis	Obsługiwane systemy operacyjne	Częstotliwość zbierania danych	Obsługa monitorowania typu Wykrywanie anomalii	Dostępność w ramach ochrony typu Standardowy lub pakiecie Zarządzanie zaawansowane
Użycie pamięci	Monitoruje ogólny poziom użycia pamięci (według wszystkich gniazd pamięci w obciążeniu).	Windows macOS	30 s	Tak	Zarządzanie zaawansowane
Szybkość transferu dysku	Monitoruje szybkość odczytu i zapisu każdego dysku fizycznego w obciążeniu.	Windows macOS	30 s	Tak	Zarządzanie zaawansowane
Wykorzystanie sieci	Monitoruje ruch przychodzący i wychodzący w przypadku każdej karty sieciowej obciążenia.	Windows macOS	30 s	Tak	Zarządzanie zaawansowane
Poziom użycia procesora przez proces	Monitoruje poziom użycia procesora przez określony proces.	Windows macOS	30 s	Nie	Zarządzanie zaawansowane
Poziom użycia pamięci przez proces	Monitoruje poziom użycia pamięci przez	Windows macOS	30 s	Nie	Zarządzanie zaawansowane

© Acronis International GmbH, 2003-2024

Monitoruj	Opis	Obsługiwane systemy operacyjne	Częstotliwość zbierania danych	Obsługa monitorowania typu Wykrywanie anomalii	Dostępność w ramach ochrony typu Standardowy lub pakiecie Zarządzanie zaawansowane
	wybrany proces.				
Szybkość transferu dysku generowanego przez proces	Monitoruje szybkość odczytu i zapisu związanego z wybranym procesem.	Windows macOS	30 s	Nie	Zarządzanie zaawansowane
Poziom użycia sieci przez proces	Monitoruje ruch przychodzący i wychodzący generowany przez wybrany proces.	Windows macOS	30 s	Nie	Zarządzanie zaawansowane
Oprogramowanie					
Status usług systemu Windows	Monitoruje status wybranej usługi systemu Windows (Uruchomiono lub Zatrzymano).	Windows	30 s	Nie	Zarządzanie zaawansowane
Status procesu	Monitoruje status wybranego procesu (Uruchomiono lub Zatrzymano).	Windows macOS	30 s	Nie	Zarządzanie zaawansowane

© Acronis International GmbH, 2003-2024

Monitoruj	Opis	Obsługiwane systemy operacyjne	Częstotliwość zbierania danych	Obsługa monitorowania typu Wykrywanie anomalii	Dostępność w ramach ochrony typu Standardowy lub pakiecie Zarządzanie zaawansowane
Zainstalowane oprogramowanie	Monitoruje instalacje, aktualizacje lub usunięcia aplikacji.	Windows macOS	24 godz.	Nie	Zarządzanie zaawansowane
System					
Ostatnie ponowne uruchomienie systemu	Monitoruje, kiedy obciążenie zostało uruchomione ponownie.	Windows macOS	1 godz.	Nie	Ochrona standardowa
Dziennik zdarzeń systemu Windows	Monitoruje konkretne krytyczne dla działalności zdarzenia w dziennikach zdarzeń systemu Windows.	Windows	10 min	Nie	Zarządzanie zaawansowane
Rozmiar plików i folderów	Monitoruje łączny rozmiar wybranych plików lub folderów.	Windows macOS	10 min	Nie	Ochrona standardowa
Zabezpieczenia					
Status usługi Windows Update	Monitoruje status usługi Windows Update obciążenia i	Windows	15 min	Nie	Zarządzanie zaawansowane

© Acronis International GmbH, 2003-2024

Monitoruj	Opis	Obsługiwane systemy operacyjne	Częstotliwość zbierania danych	Obsługa monitorowania typu Wykrywanie anomalii	Dostępność w ramach ochrony typu Standardowy lub pakiecie Zarządzanie zaawansowane
	sprawdza, czy zostały zainstalowane najnowsze aktualizacje.				
Status zapory	Monitoruje status zapory — wbudowanej lub opracowanej przez inną firmę — która jest zainstalowana na obciążeniu.	Windows macOS	5 min	Nie	Zarządzanie zaawansowane
Status oprogramowania antywirusowego	Monitoruje status oprogramowania antywirusowego — wbudowanego lub opracowanego przez inną firmę — które jest zainstalowane na obciążeniu.	Windows macOS	5 min	Nie	Zarządzanie zaawansowane
Niepowodzenia logowania	Monitoruje nieudane próby zalogowania	Windows	1 godz.	Nie	Zarządzanie zaawansowane

© Acronis International GmbH, 2003-2024

Monitoruj	Opis	Obsługiwane systemy operacyjne	Częstotliwość zbierania danych	Obsługa monitorowania typu Wykrywanie anomalii	Dostępność w ramach ochrony typu Standardowy lub pakiecie Zarządzanie zaawansowane
	się na obciążeniu.				
Status funkcji uruchamiania automatycznego	Monitoruje, czy jest włączona funkcja uruchamiania automatycznego dla wymiennych nośników pamięci.	Windows	1 godz.	Nie	Zarządzanie zaawansowane
Niestandardowe					
Niestandardowe	Monitoruje obiekty niestandardowe za pośrednictwem uruchomionych skryptów.	Windows macOS	niestandardowy	Nie	Zarządzanie zaawansowane

Ustawienia monitora Miejsce na dysku

Monitor **Miejsce na dysku** monitoruje ilość wolnego miejsca na określonym dysku obciążenia.

Uwaga
Podczas obliczania miejsca monitor stosuje bajty binarne (1024 bajty na KB, 1024 KB na MB i 1024 MB na GB) zarówno w przypadku obciążeń z systemem Windows, jak i obciążeń z systemem macOS.

Możesz skonfigurować następujące ustawienia monitora.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
Monitorowanie typu Wykrywanie progów	
Dysk	Dysk, który ma być monitorowany. Dostępne są następujące wartości. • **Dysk systemowy** —To jest wartość domyślna. • **Dowolny dysk**
Operator	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Poniżej** —To jest wartość domyślna. • **Mniejsze niż lub równe**
Próg wolnego miejsca na dysku	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą z zakresu 1–100 (%). Wartość domyślna to 20.
Uwzględnij dyski wymienne	To ustawienie jest dostępne, jeśli w polu **Dysk** ustawiono wartość **Dowolny dysk**. Wybierz to ustawienie, jeśli chcesz uwzględnić w monitorowaniu również dyski wymienne, na przykład dyski flash USB. Domyślnie to ustawienie jest wyłączone.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 30.
Monitorowanie typu Wykrywanie anomalii	
Dysk	Dysk, który ma być monitorowany. Dostępne są następujące wartości. • **Dysk systemowy** —To jest wartość domyślna. • **Dowolny dysk**
Okres szkolenia modelu	Okres, w którym system będzie szkolił modele uczenia maszynowego na podstawie danych zebranych od agentów, po czym utworzy wzorzec normalnych zachowań obciążenia. Im dłuższy będzie okres szkolenia modelu, tym dokładniejszy będzie utworzony przez system długoterminowy wzorzec zachowań. Zalecamy szkolenie modelu przez co najmniej dwadzieścia jeden dni.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	Wprowadź wartość jako liczbę całkowitą (dni). Wartość domyślna to 21.
Otrzymuj alerty o anomaliach występujących w okresie szkolenia	Jeśli wybierzesz to ustawienie, będziesz otrzymywać powiadomienia o anomaliach w okresie szkolenia modelu. Mogą to być fałszywe alerty, ponieważ w trakcie szkolenia modele mogą nie być wystarczająco dokładne. Ustawienie to jest domyślnie wybrane.
Poziom wrażliwości	Poziom wrażliwości stanowi wstępny filtr anomalii, jeśli ich wartości mieszczą się w określonym zakresie. Filtr ten działa niezależnie od algorytmu wykrywania anomalii. Ma on na celu zatrzymanie przetwarzania anomalii mieszczących się w określonym zakresie przez algorytm wykrywania anomalii. W okresie szkolenia: 1. Algorytm jest szkolony przy użyciu danych zebranych podczas szkolenia. 2. Algorytm przeprowadza wykrywanie anomalii na danych szkoleniowych. 3. Stosowany jest proces filtrowania oparty na średniej i odchyleniu standardowym. 4. Filtrowane są wszelkie anomalie znajdujące się w określonym przedziale. 5. Z pozostałych anomalnych punktów danych wybierana jest anomalia o najniższym poziomie. Poziom ten (liczba zmiennoprzecinkowa między 0 a 1) jest rejestrowany w modelu. W fazie prognozowania: 1. Algorytm prognozuje anomalie, opierając się na danych wnioskowania. 2. Przewidywane anomalie są filtrowane na podstawie średniej i odchylenia standardowego zgodnie z poziomem ważności. 3. Pozostałe anomalie są dalej filtrowane według następującej zasady: wartości powyżej poziomu progu są uznawane za anomalię, a wartości poniżej poziomu progu są uznawane za normalne zachowanie. Dostępne są następujące wartości. • **Niski** — poziom niski jest równy wartości średniej i wartości odchylenia standardowego. • **Normalny** — to jest wartość domyślna. Poziom normalny jest równy wartości średniej i dwukrotności wartości odchylenia standardowego. • **Wysoki** — poziom wysoki jest równy wartości średniej i trzykrotności wartości odchylenia standardowego.
Czas trwania anomalii	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	Wartość domyślna to 30 minut.

Ustawienia monitora Temperatura procesora

Monitor **Temperatura procesora** monitoruje temperaturę procesora obciążenia.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Monitorowanie typu Wykrywanie progów	
Temperatura procesora przekracza (°C)	Maksymalna wartość monitorowanego wskaźnika. W przypadku przekroczenia tej wartości system generuje alert. Wprowadź wartość jako liczbę całkowitą (°C). Wartość domyślna to 80.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Monitorowanie typu Wykrywanie anomalii	
Okres szkolenia modelu	Okres, w którym system będzie szkolił modele uczenia maszynowego na podstawie danych zebranych od agentów, po czym utworzy wzorzec normalnych zachowań obciążenia. Im dłuższy będzie okres szkolenia modelu, tym dokładniejszy będzie utworzony przez system długoterminowy wzorzec zachowań. Zalecamy szkolenie modelu przez co najmniej dwadzieścia jeden dni. Wprowadź wartość jako liczbę całkowitą (dni). Wartość domyślna to 21.
Poziom wrażliwości	Poziom wrażliwości stanowi wstępny filtr anomalii, jeśli ich wartości mieszczą się w określonym zakresie. Filtr ten działa niezależnie od algorytmu wykrywania anomalii. Ma on na celu zatrzymanie przetwarzania anomalii mieszczących się w określonym zakresie przez algorytm wykrywania anomalii. W okresie szkolenia: 1. Algorytm jest szkolony przy użyciu danych zebranych podczas szkolenia. 2. Algorytm przeprowadza wykrywanie anomalii na danych szkoleniowych. 3. Stosowany jest proces filtrowania oparty na średniej i

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	odchyleniu standardowym. 4. Filtrowane są wszelkie anomalie znajdujące się w określonym przedziale. 5. Z pozostałych anomalnych punktów danych wybierana jest anomalia o najniższym poziomie. Poziom ten (liczba zmiennoprzecinkowa między 0 a 1) jest rejestrowany w modelu. W fazie prognozowania: 1. Algorytm prognozuje anomalie, opierając się na danych wnioskowania. 2. Przewidywane anomalie są filtrowane na podstawie średniej i odchylenia standardowego zgodnie z poziomem ważności. 3. Pozostałe anomalie są dalej filtrowane według następującej zasady: wartości powyżej poziomu progu są uznawane za anomalię, a wartości poniżej poziomu progu są uznawane za normalne zachowanie. Dostępne są następujące wartości. • **Niski** — poziom niski jest równy wartości średniej i wartości odchylenia standardowego. • **Normalny** — to jest wartość domyślna. Poziom normalny jest równy wartości średniej i dwukrotności wartości odchylenia standardowego. • **Wysoki** — poziom wysoki jest równy wartości średniej i trzykrotności wartości odchylenia standardowego.
Czas trwania anomalii	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 15.

Ustawienia monitora Temperatura procesora graficznego

Monitor **Temperatura procesora graficznego** monitoruje temperaturę procesora graficznego obciążenia.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Monitorowanie typu Wykrywanie progów	
Temperatura	Maksymalna wartość monitorowanego wskaźnika. W przypadku

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
procesora graficznego przekracza	przekroczenia tej wartości system wykrywa anomalię. Wprowadź wartość jako liczbę całkowitą (°C). Wartość domyślna to 80.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Monitorowanie typu Wykrywanie anomalii	
Okres szkolenia modelu	Okres, w którym system będzie szkolił modele uczenia maszynowego na podstawie danych zebranych od agentów, po czym utworzy wzorzec normalnych zachowań obciążenia. Im dłuższy będzie okres szkolenia modelu, tym dokładniejszy będzie utworzony przez system długoterminowy wzorzec zachowań. Zalecamy szkolenie modelu przez co najmniej dwadzieścia jeden dni. Wprowadź wartość jako liczbę całkowitą (dni). Wartość domyślna to 21.
Poziom wrażliwości	Poziom wrażliwości stanowi wstępny filtr anomalii, jeśli ich wartości mieszczą się w określonym zakresie. Filtr ten działa niezależnie od algorytmu wykrywania anomalii. Ma on na celu zatrzymanie przetwarzania anomalii mieszczących się w określonym zakresie przez algorytm wykrywania anomalii. W okresie szkolenia: 1. Algorytm jest szkolony przy użyciu danych zebranych podczas szkolenia. 2. Algorytm przeprowadza wykrywanie anomalii na danych szkoleniowych. 3. Stosowany jest proces filtrowania oparty na średniej i odchyleniu standardowym. 4. Filtrowane są wszelkie anomalie znajdujące się w określonym przedziale. 5. Z pozostałych anomalnych punktów danych wybierana jest anomalia o najniższym poziomie. Poziom ten (liczba zmiennoprzecinkowa między 0 a 1) jest rejestrowany w modelu. W fazie prognozowania: 1. Algorytm prognozuje anomalie, opierając się na danych wnioskowania. 2. Przewidywane anomalie są filtrowane na podstawie średniej i odchylenia standardowego zgodnie z poziomem ważności. 3. Pozostałe anomalie są dalej filtrowane według następującej zasady: wartości powyżej poziomu progu są uznawane za anomalię, a wartości poniżej poziomu progu są uznawane za normalne zachowanie. Dostępne są następujące wartości. • **Niski** — poziom niski jest równy wartości średniej i wartości odchylenia

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	standardowego. • **Normalny** — to jest wartość domyślna. Poziom normalny jest równy wartości średniej i dwukrotności wartości odchylenia standardowego. • **Wysoki** — poziom wysoki jest równy wartości średniej i trzykrotności wartości odchylenia standardowego.
Czas trwania anomalii	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 15.

Ustawienia monitora Zmiany sprzętowe

Monitor **Zmiany sprzętowe** monitoruje zmiany sprzętowe, takie jak dodanie, usunięcie lub wymiana sprzętu w obciążeniu.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Komponenty sprzętowe	Wybierz komponenty sprzętowe, które mają być monitorowane pod kątem zmian. Dostępne są następujące wartości. • **Wszystkie** — To jest wartość domyślna. • **Płyta główna** • **Procesor** • **Pamięć RAM** • **Dysk** • **Procesor graficzny** • **Karta sieciowa**
Elementy do monitorowania	Określ zmiany, które mają być monitorowane w przypadku wybranych komponentów sprzętowych. Można wybrać kilka pozycji z listy. Dostępne są następujące wartości. • **Każda zmiana** —To jest wartość domyślna. • **Nowo dodane komponenty** • **Wymienione komponenty** • **Usunięte komponenty**

Ustawienia monitora Poziom użycia procesora

Monitor **Poziom użycia procesora** monitoruje łączne użycie procesora (wykorzystanie procesora) obciążenia. Jeśli obciążenie ma kilka procesorów, łączne użycie procesora będzie sumą użycia

© Acronis International GmbH, 2003-2024

każdego z tych procesorów.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Monitorowanie typu Wykrywanie progów	
Operator	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg użycia procesora	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą z zakresu 1–100 (%). Wartość domyślna to 90.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Monitorowanie typu Wykrywanie anomalii	
Okres szkolenia modelu	Okres, w którym system będzie szkolił modele uczenia maszynowego na podstawie danych zebranych od agentów, po czym utworzy wzorzec normalnych zachowań obciążenia. Im dłuższy będzie okres szkolenia modelu, tym dokładniejszy będzie utworzony przez system długoterminowy wzorzec zachowań. Zalecamy szkolenie modelu przez co najmniej dwadzieścia jeden dni. Wprowadź wartość jako liczbę całkowitą (dni). Wartość domyślna to 21.
Otrzymuj alerty o anomaliach występujących w okresie szkolenia	Jeśli wybierzesz to ustawienie, będziesz otrzymywać powiadomienia o anomaliach w okresie szkolenia modelu. Mogą to być fałszywe alerty, ponieważ w trakcie szkolenia modele mogą nie być wystarczająco dokładne. Ustawienie to jest domyślnie wybrane.
Poziom wrażliwości	Poziom wrażliwości stanowi wstępny filtr anomalii, jeśli ich wartości mieszczą się w określonym zakresie. Filtr ten działa niezależnie od algorytmu wykrywania anomalii. Ma on na celu zatrzymanie przetwarzania anomalii mieszczących się w określonym zakresie przez algorytm

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	wykrywania anomalii. W okresie szkolenia: 1. Algorytm jest szkolony przy użyciu danych zebranych podczas szkolenia. 2. Algorytm przeprowadza wykrywanie anomalii na danych szkoleniowych. 3. Stosowany jest proces filtrowania oparty na średniej i odchyleniu standardowym. 4. Filtrowane są wszelkie anomalie znajdujące się w określonym przedziale. 5. Z pozostałych anomalnych punktów danych wybierana jest anomalia o najniższym poziomie. Poziom ten (liczba zmiennoprzecinkowa między 0 a 1) jest rejestrowany w modelu. W fazie prognozowania: 1. Algorytm prognozuje anomalie, opierając się na danych wnioskowania. 2. Przewidywane anomalie są filtrowane na podstawie średniej i odchylenia standardowego zgodnie z poziomem ważności. 3. Pozostałe anomalie są dalej filtrowane według następującej zasady: wartości powyżej poziomu progu są uznawane za anomalię, a wartości poniżej poziomu progu są uznawane za normalne zachowanie. Dostępne są następujące wartości. • **Niski** — poziom niski jest równy wartości średniej i wartości odchylenia standardowego. • **Normalny** — to jest wartość domyślna. Poziom normalny jest równy wartości średniej i dwukrotności wartości odchylenia standardowego. • **Wysoki** — poziom wysoki jest równy wartości średniej i trzykrotności wartości odchylenia standardowego.
Czas trwania anomalii	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 15.

Ustawienia monitora Poziom użycia pamięci

Monitor **Poziom użycia pamięci** monitoruje ogólny poziom użycia pamięci w przypadku wszystkich modułów pamięci w obciążeniu.

Możesz skonfigurować następujące ustawienia monitora.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
Monitorowanie typu Wykrywanie progów	
Operator	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg użycia pamięci	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą z zakresu 1–100 (%). Wartość domyślna to 90.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Monitorowanie typu Wykrywanie anomalii	
Okres szkolenia modelu	Okres, w którym system będzie szkolił modele uczenia maszynowego na podstawie danych zebranych od agentów, po czym utworzy wzorzec normalnych zachowań obciążenia. Im dłuższy będzie okres szkolenia modelu, tym dokładniejszy będzie utworzony przez system długoterminowy wzorzec zachowań. Zalecamy szkolenie modelu przez co najmniej dwadzieścia jeden dni. Wprowadź wartość jako liczbę całkowitą (dni). Wartość domyślna to 21.
Otrzymuj alerty o anomaliach występujących w okresie szkolenia	Jeśli wybierzesz to ustawienie, będziesz otrzymywać powiadomienia o anomaliach w okresie szkolenia modelu. Mogą to być fałszywe alerty, ponieważ w trakcie szkolenia modele mogą nie być wystarczająco dokładne. Ustawienie to jest domyślnie wybrane.
Poziom wrażliwości	Poziom wrażliwości stanowi wstępny filtr anomalii, jeśli ich wartości mieszczą się w określonym zakresie. Filtr ten działa niezależnie od algorytmu wykrywania anomalii. Ma on na celu zatrzymanie przetwarzania anomalii mieszczących się w określonym zakresie przez algorytm wykrywania anomalii. W okresie szkolenia: 1. Algorytm jest szkolony przy użyciu danych zebranych podczas

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	szkolenia. 2. Algorytm przeprowadza wykrywanie anomalii na danych szkoleniowych. 3. Stosowany jest proces filtrowania oparty na średniej i odchyleniu standardowym. 4. Filtrowane są wszelkie anomalie znajdujące się w określonym przedziale. 5. Z pozostałych anomalnych punktów danych wybierana jest anomalia o najniższym poziomie. Poziom ten (liczba zmiennoprzecinkowa między 0 a 1) jest rejestrowany w modelu. W fazie prognozowania: 1. Algorytm prognozuje anomalie, opierając się na danych wnioskowania. 2. Przewidywane anomalie są filtrowane na podstawie średniej i odchylenia standardowego zgodnie z poziomem ważności. 3. Pozostałe anomalie są dalej filtrowane według następującej zasady: wartości powyżej poziomu progu są uznawane za anomalię, a wartości poniżej poziomu progu są uznawane za normalne zachowanie. Dostępne są następujące wartości. • **Niski** — poziom niski jest równy wartości średniej i wartości odchylenia standardowego. • **Normalny** — to jest wartość domyślna. Poziom normalny jest równy wartości średniej i dwukrotności wartości odchylenia standardowego. • **Wysoki** — poziom wysoki jest równy wartości średniej i trzykrotności wartości odchylenia standardowego.
Czas trwania anomalii	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 30 minut.

Ustawienia monitora Szybkość transferu dysku

Monitor **Szybkość transferu dysku** monitoruje szybkość odczytu i zapisu każdego dysku fizycznego w obciążeniu.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Monitorowanie typu Wykrywanie progów	
Elementy do monitorowania	Wybierz szybkość, która ma być monitorowana. Dostępne są następujące wartości.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	• **Szybkość odczytu i zapisu**. To jest wartość domyślna. • **Szybkość odczytu** • **Szybkość zapisu**
Operator szybkości odczytu	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad**. To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg szybkości odczytu	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb/s). Wartość domyślna to 0 kb/s.
Okres szybkości odczytu	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Operator szybkości zapisu	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg szybkości zapisu	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb/s). Wartość domyślna to 0 kb/s.
Okres szybkości zapisu	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Monitorowanie typu Wykrywanie anomalii	

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
Okres szkolenia modelu	Okres, w którym system będzie szkolił modele uczenia maszynowego na podstawie danych zebranych od agentów, po czym utworzy wzorzec normalnych zachowań obciążenia. Im dłuższy będzie okres szkolenia modelu, tym dokładniejszy będzie utworzony przez system długoterminowy wzorzec zachowań. Zalecamy szkolenie modelu przez co najmniej dwadzieścia jeden dni. Wprowadź wartość jako liczbę całkowitą (dni). Wartość domyślna to 21.
Otrzymuj alerty o anomaliach występujących w okresie szkolenia	Jeśli wybierzesz to ustawienie, będziesz otrzymywać powiadomienia o anomaliach w okresie szkolenia modelu. Mogą to być fałszywe alerty, ponieważ w trakcie szkolenia modele mogą nie być wystarczająco dokładne. Ustawienie to jest domyślnie wybrane.
Elementy do monitorowania	Wybierz szybkość, która ma być monitorowana. Dostępne są następujące wartości. • **Szybkość odczytu i zapisu**. To jest wartość domyślna. • **Szybkość odczytu** • **Szybkość zapisu**
Poziom wrażliwości	Poziom wrażliwości stanowi wstępny filtr anomalii, jeśli ich wartości mieszczą się w określonym zakresie. Filtr ten działa niezależnie od algorytmu wykrywania anomalii. Ma on na celu zatrzymanie przetwarzania anomalii mieszczących się w określonym zakresie przez algorytm wykrywania anomalii. W okresie szkolenia: 1. Algorytm jest szkolony przy użyciu danych zebranych podczas szkolenia. 2. Algorytm przeprowadza wykrywanie anomalii na danych szkoleniowych. 3. Stosowany jest proces filtrowania oparty na średniej i odchyleniu standardowym. 4. Filtrowane są wszelkie anomalie znajdujące się w określonym przedziale. 5. Z pozostałych anomalnych punktów danych wybierana jest anomalia o najniższym poziomie. Poziom ten (liczba zmiennoprzecinkowa między 0 a 1) jest rejestrowany w modelu. W fazie prognozowania: 1. Algorytm prognozuje anomalie, opierając się na danych wnioskowania. 2. Przewidywane anomalie są filtrowane na podstawie średniej i odchylenia standardowego zgodnie z poziomem ważności.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	3. Pozostałe anomalie są dalej filtrowane według następującej zasady: wartości powyżej poziomu progu są uznawane za anomalię, a wartości poniżej poziomu progu są uznawane za normalne zachowanie. Dostępne są następujące wartości. • **Niski** — poziom niski jest równy wartości średniej i wartości odchylenia standardowego. • **Normalny** — to jest wartość domyślna. Poziom normalny jest równy wartości średniej i dwukrotności wartości odchylenia standardowego. • **Wysoki** — poziom wysoki jest równy wartości średniej i trzykrotności wartości odchylenia standardowego.
Czas trwania anomalii (szybkość odczytu)	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 25.
Czas trwania anomalii (szybkość zapisu)	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 25.

Ustawienia monitora Wykorzystanie sieci

Monitor **Wykorzystanie sieci** monitoruje ruch przychodzący i wychodzący w przypadku każdej karty sieciowej obciążenia.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Monitorowanie typu Wykrywanie progów	
Kierunek ruchu	Kierunek ruchu, który ma być monitorowany. Dostępne są następujące wartości. • **Ruch przychodzący i wychodzący**. To jest wartość domyślna. • **Ruch przychodzący** • **Ruch wychodzący**
Operator ruchu przychodzącego	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	• **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg ruchu przychodzącego	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb/s). Wartość domyślna to 0 kb/s.
Okres ruchu przychodzącego	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Operator ruchu wychodzącego	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg ruchu wychodzącego	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb/s). Wartość domyślna to 0 kb/s.
Okres ruchu wychodzącego	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Monitorowanie typu Wykrywanie anomalii	
Okres szkolenia modelu	Okres, w którym system będzie szkolił modele uczenia maszynowego na podstawie danych zebranych od agentów, po czym utworzy wzorzec normalnych zachowań obciążenia. Im dłuższy będzie okres szkolenia modelu, tym dokładniejszy będzie utworzony przez system długoterminowy wzorzec zachowań. Zalecamy szkolenie modelu przez co najmniej dwadzieścia jeden dni. Wprowadź wartość jako liczbę całkowitą (dni). Wartość domyślna to 21.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
Otrzymuj alerty o anomaliach występujących w okresie szkolenia	Jeśli wybierzesz to ustawienie, będziesz otrzymywać powiadomienia o anomaliach w okresie szkolenia modelu. Mogą to być fałszywe alerty, ponieważ w trakcie szkolenia modele mogą nie być wystarczająco dokładne. Ustawienie to jest domyślnie wybrane.
Kierunek ruchu	• **Ruch przychodzący i wychodzący**. To jest wartość domyślna. • **Ruch przychodzący** • **Ruch wychodzący**
Poziom wrażliwości	Poziom wrażliwości stanowi wstępny filtr anomalii, jeśli ich wartości mieszczą się w określonym zakresie. Filtr ten działa niezależnie od algorytmu wykrywania anomalii. Ma on na celu zatrzymanie przetwarzania anomalii mieszczących się w określonym zakresie przez algorytm wykrywania anomalii. W okresie szkolenia: 1. Algorytm jest szkolony przy użyciu danych zebranych podczas szkolenia. 2. Algorytm przeprowadza wykrywanie anomalii na danych szkoleniowych. 3. Stosowany jest proces filtrowania oparty na średniej i odchyleniu standardowym. 4. Filtrowane są wszelkie anomalie znajdujące się w określonym przedziale. 5. Z pozostałych anomalnych punktów danych wybierana jest anomalia o najniższym poziomie. Poziom ten (liczba zmiennoprzecinkowa między 0 a 1) jest rejestrowany w modelu. W fazie prognozowania: 1. Algorytm prognozuje anomalie, opierając się na danych wnioskowania. 2. Przewidywane anomalie są filtrowane na podstawie średniej i odchylenia standardowego zgodnie z poziomem ważności. 3. Pozostałe anomalie są dalej filtrowane według następującej zasady: wartości powyżej poziomu progu są uznawane za anomalię, a wartości poniżej poziomu progu są uznawane za normalne zachowanie. Dostępne są następujące wartości. • **Niski** — poziom niski jest równy wartości średniej i wartości odchylenia standardowego. • **Normalny** — to jest wartość domyślna. Poziom normalny jest równy wartości średniej i dwukrotności wartości odchylenia standardowego. • **Wysoki** — poziom wysoki jest równy wartości średniej i trzykrotności

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	wartości odchylenia standardowego.
Czas trwania anomalii (przychodzący)	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 25.
Czas trwania anomalii (wychodzący)	System wygeneruje alert o wykrytej anomalii tylko wtedy, gdy odbiegające od normy zachowanie będzie się utrzymywać przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 25.

Ustawienia monitora Poziom użycia procesora przez proces

Monitor **Poziom użycia procesora przez proces** monitoruje wykorzystanie procesora przez wybrany proces. Jeśli istnieje więcej niż jedna instancja tego samego procesu, system będzie monitorował łączne wykorzystanie przez wszystkie instancje procesu i wygeneruje alert, gdy zostaną spełnione warunki.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Nazwa procesu	Nazwa procesu, który ma być monitorowany. Wprowadź nazwę procesu bez rozszerzenia.
Operator	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą z zakresu 1–100 (%). Wartość domyślna to 90.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.

Ustawienia monitora Poziom użycia pamięci przez proces

Monitor **Poziom użycia pamięci przez proces** monitoruje wykorzystanie pamięci operacyjnej przez wybrany proces. Jeśli istnieje więcej niż jedna instancja tego samego procesu, system będzie monitorował łączne wykorzystanie przez wszystkie instancje procesu i wygeneruje alert, gdy zostaną spełnione warunki.

Uwaga
Agenty wykorzystują całkowity zestaw roboczy procesu (prywatny i udostępniony) w celu oszacowania rozmiaru użycia pamięci przez proces. Dlatego rozmiar wyświetlany na widżecie może się różnić od rozmiaru użycia pamięci wyświetlanego w Menedżerze zadań systemu Windows (prywatny zestaw roboczy).

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Nazwa procesu	Nazwa procesu, który ma być monitorowany. Wprowadź nazwę procesu bez rozszerzenia.
Operator	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb). Wartość domyślna to 1.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.

© Acronis International GmbH, 2003-2024

Ustawienia monitora Szybkość transferu dysku generowanego przez proces

Monitor **Szybkość transferu dysku generowanego przez proces** monitoruje szybkość odczytu i zapisu związanego z wybranym procesem. Jeśli istnieje więcej niż jedna instancja tego samego procesu, system będzie monitorował łączne wykorzystanie przez wszystkie instancje procesu i wygeneruje alert, gdy zostaną spełnione warunki.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Nazwa procesu	Nazwa procesu, który ma być monitorowany. Wprowadź nazwę procesu bez rozszerzenia.
Elementy do monitorowania	Szybkość, która ma być monitorowana. Dostępne są następujące wartości. • **Szybkość odczytu i zapisu**. To jest wartość domyślna. • **Szybkość odczytu** • **Szybkość zapisu**
Operator szybkości odczytu	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg szybkości odczytu	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb/s). Wartość domyślna to 0 kb/s.
Okres szybkości odczytu	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Operator szybkości zapisu	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	• **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg szybkości zapisu	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb/s). Wartość domyślna to 0 kb/s.
Okres szybkości zapisu	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.

Ustawienia monitora Poziom użycia sieci przez proces

Monitor **Poziom użycia sieci przez proces** monitoruje ruch przychodzący i wychodzący generowany przez wybrany proces. Jeśli istnieje więcej niż jedna instancja tego samego procesu, system będzie monitorował łączne wykorzystanie przez wszystkie instancje procesu i wygeneruje alert, gdy zostaną spełnione warunki w przypadku wszystkich instancji.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Nazwa procesu	Nazwa procesu, który ma być monitorowany. Wprowadź nazwę procesu bez rozszerzenia.
Kierunek ruchu	Kierunek ruchu, który ma być monitorowany. Dostępne są następujące wartości. • **Ruch przychodzący i wychodzący**. To jest wartość domyślna. • **Ruch przychodzący** • **Ruch wychodzący**
Operator ruchu przychodzącego	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg ruchu	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
przychodzącego	monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb/s). Wartość domyślna to 0 kb/s.
Okres ruchu przychodzącego	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.
Operator ruchu wychodzącego	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Większe niż lub równe** • **Poniżej** • **Mniejsze niż lub równe**
Próg ruchu wychodzącego	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (kb/s). Wartość domyślna to 0 kb/s.
Okres ruchu wychodzącego	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 5.

Ustawienia monitora Status usług systemu Windows

Monitor **Status usług systemu Windows** monitoruje, czy wybrana usługa systemu Windows jest uruchomiona czy zatrzymana.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Nazwa usługi	Nazwa usługi Windows, która ma być monitorowana. Możesz wybrać nazwę usługi z listy usług systemu Windows. Lista jest wypełniana przez wszystkich agentów dzierżawcy po pomyślnym zakończeniu skanowania w celu inwentaryzacji oprogramowania na obciążeniach. Możesz też dodać nazwę usługi, której nie ma na liście. Jest to jedyna dostępna opcja, jeśli nie przeprowadzono skanowania w celu inwentaryzacji oprogramowania

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	na obciążeniach.
Status usługi	Jeśli usługa będzie mieć wybrany status, system wygeneruje zdarzenie. Dostępne są następujące wartości. • **Uruchomiono** • **Zatrzymano** —To jest wartość domyślna.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 1.

Ustawienia monitora Status procesu

Monitor **Status procesu** monitoruje, czy wybrany proces jest uruchomiony czy zatrzymany. Jeśli istnieje więcej niż jedna instancja tego samego procesu, system będzie monitorował każdą instancję procesu i wygeneruje alert, gdy zostaną spełnione warunki w przypadku wszystkich instancji procesu.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Nazwa procesu	Nazwa procesu, który ma być monitorowany. Wprowadź nazwę pliku wykonywalnego bez rozszerzenia.
Status procesu	Jeśli proces będzie mieć wybrany status, system wygeneruje zdarzenie. Dostępne są następujące wartości. • **Uruchomiono** • **Zatrzymano** —To jest wartość domyślna.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–60 (minut). Wartość domyślna to 1.

Ustawienia monitora Zainstalowane oprogramowanie

Monitor **Zainstalowane oprogramowanie** monitoruje instalacje, aktualizacje lub usunięcia aplikacji na obciążeniu.

Możesz skonfigurować następujące ustawienia monitora.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
Oprogramowanie do monitorowania	Określ oprogramowanie, które ma być monitorowane. Dostępne są następujące wartości. • **Każde oprogramowanie** —To jest wartość domyślna. • **Konkretne oprogramowanie**
Nazwy oprogramowania	To ustawienie staje się dostępne po wybraniu wartości **Konkretne oprogramowanie** w polu **Oprogramowanie do monitorowania**. Wprowadź nazwę co najmniej jednej aplikacji. Możesz wybrać nazwę aplikacji z listy usług systemu Windows. Lista jest wypełniana przez wszystkich agentów dzierżawcy po pomyślnym zakończeniu skanowania w celu inwentaryzacji oprogramowania na obciążeniach. Możesz też dodać nazwę aplikacji, której nie ma na liście. Jest to jedyna dostępna opcja, jeśli nie przeprowadzono skanowania w celu inwentaryzacji oprogramowania na obciążeniach.
Status instalacji	Określ, czy chcesz monitorować zainstalowane, niezainstalowane czy zaktualizowane oprogramowanie. Dostępne są następujące wartości. • **Zainstalowane** — To jest wartość domyślna. w przypadku wybrania tej wartości monitor wygeneruje alert, gdy na obciążeniu zostanie zainstalowana nowa aplikacja. • **Zaktualizowane** — w przypadku wybrania tej wartości monitor wygeneruje alert, gdy na obciążeniu zostanie zaktualizowana aplikacja. • **Niezainstalowane** — w przypadku wybrania tej wartości monitor wygeneruje alert, gdy aplikacja zostanie odinstalowana na maszynie lub nie jest na maszynie dostępna.

Ustawienia monitora Ostatnie ponowne uruchomienie systemu

Monitor **Ostatnie ponowne uruchomienie systemu** monitoruje, kiedy obciążenie zostało ostatni raz uruchomione ponownie.

Możesz skonfigurować następujące ustawienie monitora.

Ustawienie	Opis
Obciążenie nie zostało uruchomione ponownie przez	Czas (liczba dni), który upłynął od ostatniego ponownego uruchomienia obciążenia. Jeśli obciążenie nie zostało uruchomione ponownie przez czas dłuższy niż wskazany, system wygeneruje alert. Wprowadź wartość jako liczbę całkowitą z zakresu 1–180 (dni). Wartość domyślna to 30.

© Acronis International GmbH, 2003-2024

Ustawienia monitora Dziennik zdarzeń systemu Windows

Monitor **Dziennik zdarzeń systemu Windows** monitoruje konkretne krytyczne dla działalności zdarzenia w dziennikach zdarzeń systemu Windows.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Nazwa dziennika zdarzeń	Wybierz dziennik zdarzeń z listy dzienników zdarzeń systemu Windows dostępnych w Podglądzie zdarzeń systemu Windows. Dostępne są następujące wartości. • **Dowolne** —To jest wartość domyślna. • **Aplikacja** • **Zabezpieczenia** • **System**
Źródło zdarzenia	Nazwa źródła zdarzeń Możesz wybrać wartość z listy źródeł zdarzeń, które są zbierane od wszystkich agentów dzierżawcy, lub ręcznie wprowadzić nową nazwę źródła. Jeśli w przypadku danego dzierżawcy wyłączono skanowanie w celu inwentaryzacji oprogramowania, lista źródeł zdarzeń będzie pusta.
Tryb dopasowania	W tym polu można określić, czy ustawienia **Identyfikatory zdarzeń**, **Typ zdarzenia** i **Opis zdarzenia** mają zostać połączone za pomocą operatora **Dowolne** lub **Wszystkie**. Dostępne są następujące wartości. • **Dowolne** —To jest wartość domyślna. alert zostanie wygenerowany w przypadku dopasowania do dowolnego z wybranych kryteriów. • **Wszystkie** — alert zostanie wygenerowany w przypadku dopasowania do wszystkich wybranych kryteriów.
Identyfikatory zdarzeń	Wprowadź identyfikatory zdarzeń, rozdzielając je przecinkami. Jeśli system znajdzie w dzienniku zdarzeń dowolny z kodów zdarzenia wprowadzonych w tym polu, wygeneruje alert.
Typ zdarzenia	Wybierz typy zdarzeń, które mają być monitorowane. Dostępne są następujące wartości. • **Dowolne** —To jest wartość domyślna. • **Błąd** • **Ostrzeżenie** • **Informacja** • **Sukces-inspekcja**

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	• **Niepowodzenie-inspekcja**
Opis zdarzenia	Konkretne słowa kluczowe lub frazy w opisie zdarzenia, które mają zostać wyszukane. Każde wprowadzane słowo kluczowe lub fraza muszą być ujęte w cudzysłowy i rozdzielone przecinkami. Jeśli system znajdzie którekolwiek z wprowadzonych słów kluczowych lub fraz, wygeneruje alert.
Liczba wystąpień	Minimalna liczba zdarzeń w dzienniku, które muszą wystąpić w danym okresie, aby system wygenerował alert. Wprowadź wartość jako liczbę całkowitą z zakresu 1–1000.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą i wybierz jednostkę: minuty lub godziny. Wartość domyślna to 60 minut.

Ustawienia monitora Rozmiar plików i folderów

Monitor **Rozmiar plików i folderów** monitoruje łączny rozmiar wybranych plików i folderów.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Pliki lub foldery do monitorowania	Ścieżki do plików lub folderów, które mają być monitorowane. Można też podać ścieżki do plików lub folderów, które nie mają być monitorowane. Można używać następujących znaków wieloznacznych. • * — zastępuje zero lub więcej znaków w nazwie pliku bądź folderu • ? — zastępuje dokładnie jeden znak w nazwie pliku lub folderu W przypadku obciążeń z systemem Windows: • Pełna ścieżka powinna się zaczynać od litery dysku, po której następuje separator :\. • Jako znaku separatora można użyć ukośnika lub ukośnika odwrotnego. • Nazwa pliku lub folderu nie może się kończyć spacją ani kropką. W przypadku obciążeń z systemem macOS: • Pełna ścieżka powinna się zaczynać od katalogu głównego. • Jako znaku separatora można użyć ukośnika. • Nazwa pliku lub folderu nie może się kończyć spacją ani kropką. Nie trzeba podawać konkretnej lokalizacji w przypadku filtrów wykluczeń. Pliki wprowadzone bez konkretnej lokalizacji zostaną wykluczone w monitorowanych folderach.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
Operator	Operator jest funkcją warunkową, która definiuje sposób pomiaru wyników wskaźnika. Dostępne są następujące wartości. • **Ponad** —To jest wartość domyślna. • **Poniżej**
Wartość progu	Wartość progu i wartość w polu **Operator** wyznaczają normalne wyniki monitorowanego wskaźnika. Gdy wartość monitorowanego wskaźnika wykracza poza normę, system generuje alert. Wprowadź wartość jako liczbę całkowitą (MB).
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 10–60 (minut). Wartość domyślna to 10.

Ustawienia monitora Status usługi Windows Update

Monitor **Status usługi Windows Update** monitoruje status usługi Windows Update obciążenia i sprawdza, czy zostały zainstalowane najnowsze aktualizacje.

Jeśli ten monitor zostanie włączony, system wygeneruje alert w następujących przypadkach.

- Usługa Windows Update jest wyłączona na obciążeniu.
- Usługa Windows Update jest włączona na obciążeniu, ale nie zostały zainstalowane najnowsze aktualizacje.

Ustawienia monitora Status zapory

Monitor **Status zapory** monitoruje status zapory — wbudowanej lub opracowanej przez inną firmę — która jest zainstalowana na obciążeniu.

Jeśli ten monitor zostanie włączony, system wygeneruje alert w następujących przypadkach.

- Wbudowana zapora systemu operacyjnego (zapora Windows Defender lub zapora systemu macOS) jest wyłączona i nie jest uruchomiona żadna zapora innej firmy.
- Zapora Windows Defender jest wyłączona dla sieci publicznych.
- Zapora Windows Defender jest wyłączona dla sieci prywatnych.
- Zapora Windows Defender jest wyłączona dla sieci z domenami.

Ustawienia monitora Niepowodzenia logowania

Monitor **Niepowodzenia logowania** monitoruje nieudane próby zalogowania się na obciążeniu.

Możesz skonfigurować następujące ustawienia monitora.

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
Próg nieudanych prób zalogowania się	Wartość progu wyznacza granice normalnych wyników monitorowanego wskaźnika. Przekroczenie wartości progu oznacza wartość poza normą. Wprowadź wartość jako liczbę całkowitą. Wartość domyślna to 60.
Okres	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas. Wprowadź wartość jako liczbę całkowitą z zakresu 1–24 i wybierz jednostkę: godziny lub dni. Wartość domyślna to 12.

Ustawienia monitora Status oprogramowania antywirusowego

Monitor **Status oprogramowania antywirusowego** monitoruje wbudowane lub opracowane przez inną firmę oprogramowanie antywirusowe zainstalowane na obciążeniu.

Jeśli ten monitor zostanie włączony, system wygeneruje alert, gdy wykryje jedną z poniższych sytuacji.

- Oprogramowanie antywirusowe nie jest zainstalowane na obciążeniu.
- Oprogramowanie antywirusowe jest zainstalowane, ale nie uruchomione.
- Oprogramowanie antywirusowe jest zainstalowane i uruchomione, ale definicje antywirusowe są nieaktualne.

Uwaga
Warunek ten jest sprawdzany w przypadku systemów operacyjnych Windows i Windows Server.

System operacyjny	Obsługiwane oprogramowanie antywirusowe
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton AntiVirus • SentinelOne • Trend Micro Endpoint Security z Apex One • Trend Micro Worry-Free Business • McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud

© Acronis International GmbH, 2003-2024

System operacyjny	Obsługiwane oprogramowanie antywirusowe
	• BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **Uwaga** Monitor może współpracować z jeszcze innymi aplikacjami antywirusowymi, ale nie jest to gwarantowane.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus for Mac • Sophos Home • Sophos Endpoint Protection • Avast Security for Mac • AVG AntiVirus for Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus for Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac

© Acronis International GmbH, 2003-2024

System operacyjny	Obsługiwane oprogramowanie antywirusowe
	Uwaga Monitor może współpracować z jeszcze innymi aplikacjami antywirusowymi, ale nie jest to gwarantowane.

Ustawienia monitora Status funkcji uruchamiania automatycznego

Monitor **Status funkcji uruchamiania automatycznego** monitoruje, czy jest włączona funkcja uruchamiania automatycznego dla wymiennych nośników pamięci.

Ze względów bezpieczeństwa zalecamy wyłączenie na obciążeniu funkcji uruchamiania automatycznego dla wymiennych nośników pamięci. Jeśli ta funkcja jest włączona, system wygeneruje alert.

Ustawienia monitora Niestandardowe

Monitor **Niestandardowe** monitoruje obiekty niestandardowe za pośrednictwem uruchomionych skryptów.

Możesz skonfigurować następujące ustawienia monitora.

Ustawienie	Opis
Skrypt do uruchomienia	Lista predefiniowanych skryptów z repozytorium skryptów.
Harmonogram	Czas uruchomienia skryptu i opcjonalnie dodatkowe warunki, które muszą zostać spełnione, aby został uruchomiony skrypt. Dostępne są następujące wartości. • **Zaplanuj według czasu** — skrypt zostanie uruchomiony dokładnie w określonym czasie: godzinach, dniach, tygodniach lub miesiącach. To jest wartość domyślna. **Typ harmonogramu** — **Godzina**, **Dzień** lub **Miesiąc** **Uruchom w podanym okresie** — zakres czasu, w którym ma zostać uruchomiony skrypt. • **Gdy użytkownik zaloguje się w systemie** — skrypt będzie uruchamiany, gdy użytkownik zaloguje się na obciążeniu. • **Gdy użytkownik wyloguje się z systemu** — skrypt będzie uruchamiany, gdy użytkownik wyloguje się na obciążeniu. • **Podczas uruchamiania systemu** — skrypt będzie uruchamiany podczas uruchamiania systemu operacyjnego obciążenia. • **Gdy system jest wyłączany** — skrypt będzie uruchamiany w przypadku wyłączenia obciążenia. • **Gdy system przechodzi w tryb online** — skrypt będzie uruchamiany,

© Acronis International GmbH, 2003-2024

Ustawienie	Opis
	gdy obciążenie przejdzie w tryb online. **Warunki rozpoczęcia** — zadanie zostanie wykonane w określonym czasie lub po określonym zdarzeniu tylko wtedy, gdy zostanie spełniony odpowiedni warunek. W przypadku wybrania wielu warunków zadanie zostanie rozpoczęte dopiero wtedy, gdy zostaną spełnione wszystkie te warunki. Domyślnie wybrany jest warunek **Zapobiegaj trybowi uśpienia lub hibernacji, aby rozpocząć zaplanowane zadanie**. **Jeśli warunki uruchomienia nie zostaną spełnione, zadanie i tak zostanie uruchomione po** — ten warunek jest domyślnie włączony. Wartość domyślna to 1 godzina.
Konto na potrzeby wykonania skryptu	Konto, na którym zostanie uruchomiony skrypt. Dostępne są następujące wartości. • **Konto systemowe** — To jest wartość domyślna. • **Aktualnie zalogowane konto**
Maksymalny czas trwania	Maksymalny czas, przez który skrypt może działać na obciążeniu. Jeśli skrypt nie zostanie ukończony w tym czasie, operacja zakończy się niepowodzeniem. Wprowadź wartość jako liczbę całkowitą z zakresu 1–1440 (minut). Wartość domyślna to 3 minuty.
Zasady wykonywania w programie PowerShell	Zasady wykonywania w programie PowerShell. Dostępne są następujące wartości. • **Undefined** • **AllSigned** • **Bypass** — To jest wartość domyślna. • **RemoteSigned** • **Restricted** • **Unrestricted** Dodatkowe informacje na temat tych wartości można znaleźć w dokumentacji firmy Microsoft.

Plany monitorowania

Plany monitorowania to plany, które stosuje się do zarządzanych obciążeń, aby włączyć i skonfigurować funkcję monitorowania.

Jeśli do danego obciążenia nie zostanie zastosowany żaden plan monitorowania, to funkcja monitorowania nie będzie dostępna w przypadku tego obciążenia.

© Acronis International GmbH, 2003-2024

Uwaga
Dostępność ustawień, które można skonfigurować w planie monitorowania, zależy od pakietu usługi zastosowanego do danego dzierżawcy. Aby uzyskać dostęp do wszystkich ustawień, należy aktywować pakiet Zarządzanie zaawansowane.

Tworzenie planu monitorowania

Możesz utworzyć plan monitorowania, a następnie dodać do niego obciążenia, aby skonfigurować funkcję monitorowania na obciążeniach zarządzanych.

Wymagania wstępne

Wersja agenta zainstalowana na obciążeniu obsługuje funkcję monitorowania.

Aby utworzyć plan monitorowania

W sekcji Plany monitorowania

1. W konsoli Ochrona przejdź do sekcji **Zarządzanie** > **Plany monitorowania**.
2. Utwórz plan monitorowania przy użyciu jednej z dwóch opcji.
   - Jeśli na liście nie ma żadnych planów monitorowania, kliknij **Utwórz**.
   - Jeśli na liście są plany monitorowania, kliknij **Utwórz plan**.
3. W oknie **Utwórz plan monitorowania** w zależności od tego, czy dla dzierżawcy jest włączony pakiet Zarządzanie zaawansowane, wykonaj następujące czynności:
   - Jeśli dzierżawca korzysta z ochrony na poziomie Standardowy, do planu monitorowania zostaną automatycznie dodane następujące cztery monitory: Miejsce na dysku, Zmiany sprzętowe, Ostatnie ponowne uruchomienie systemu oraz Rozmiar plików i folderów.
   - Jeśli dla dzierżawcy jest włączony pakiet Zarządzanie zaawansowane, wybierz jedną z opcji szablonu, a następnie kliknij **Dalej**.

Opcja	Opis
Zalecane	Wybierz tę opcję, aby utworzyć plan monitorowania z domyślną konfiguracją monitorowania.
Niestandardowe	Użyj tej opcji, aby utworzyć plan monitorowania od podstaw.

4. [Opcjonalnie] Aby zmienić domyślną nazwę planu, kliknij ikonę ołówka, wpisz nazwę planu, a następnie kliknij **OK**.
5. [Opcjonalnie] Aby dodać monitor do planu, kliknij **Dodaj monitor**, kliknij monitor na liście, a następnie kliknij **Dodaj**.

© Acronis International GmbH, 2003-2024

Uwaga
Ustawienia monitora zostaną automatycznie wypełnione wartościami domyślnymi.
Do planu monitorowania można dodać maksymalnie 3 monitory tego samego typu i maksymalnie 30 monitorów łącznie.

6. [Opcjonalnie] Na ekranie parametrów monitora zmień domyślne ustawienia monitora i alertów, a następnie kliknij **Gotowe**.

Uwaga
W przypadku każdego monitora można skonfigurować inne ustawienia. Dodatkowe informacje można znaleźć w sekcjach "Konfigurowalne monitory" (s. 1121) i "Konfigurowanie alertów dotyczących monitorowania" (s. 1168).

7. [Opcjonalnie] Aby usunąć monitor, kliknij ikonę kosza, a następnie kliknij **Usuń**.
8. [Opcjonalnie] Aby dodać obciążenia do planu:
   a. Kliknij **Dodaj obciążenia**.
   b. Wybierz obciążenia, a następnie kliknij **Dodaj**.
   c. Jeśli występują problemy z kompatybilnością, które chcesz rozwiązać, wykonaj procedurę opisaną w sekcji "Rozwiązywanie problemów z kompatybilnością dotyczących planów monitorowania" (s. 1166).
9. Kliknij **Utwórz**.

W sekcji Wszystkie urządzenia

1. W konsoli Ochrona przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie, do którego chcesz zastosować plan monitorowania.
3. Kliknij **Chroń**.
4. W zależności od tego, czy do obciążenia zastosowano plan monitorowania, wykonaj następujące czynności:
   - Jeśli plan monitorowania jest już zastosowany do obciążenia, kliknij **Utwórz plan**, a następnie wybierz **Monitorowanie**.
   - Jeśli do obciążenia nie zastosowano żadnego planu monitorowania, kliknij kolejno **Dodaj plan**, **Utwórz plan** i **Monitorowanie**.
5. W oknie **Utwórz plan monitorowania** wybierz jedną z opcji szablonu, a następnie kliknij **Dalej**.

Opcja	Opis
Zalecane	Wybierz tę opcję, aby utworzyć plan monitorowania z domyślną konfiguracją monitorowania.
Niestandardowe	Użyj tej opcji, aby utworzyć plan monitorowania od podstaw.

6. [Opcjonalnie] Aby zmienić domyślną nazwę planu, kliknij ikonę ołówka, wpisz nazwę planu, a następnie kliknij **OK**.

© Acronis International GmbH, 2003-2024

7. [Opcjonalnie] Jeśli chcesz zmienić domyślne ustawienia monitora i alertów, skonfiguruj nowe wartości, a następnie kliknij **Gotowe**.

   Uwaga
   Do planu monitorowania można dodać maksymalnie 3 monitory tego samego typu i maksymalnie 30 monitorów łącznie.

8. [Opcjonalnie] Na ekranie parametrów monitora zmień domyślne ustawienia monitora i alertów, a następnie kliknij **Gotowe**.

   Uwaga
   W przypadku każdego monitora można skonfigurować inne ustawienia. Dodatkowe informacje można znaleźć w sekcjach "Konfigurowalne monitory" (s. 1121) i "Konfigurowanie alertów dotyczących monitorowania" (s. 1168).

9. [Opcjonalnie] Aby usunąć monitor, kliknij ikonę kosza, a następnie kliknij **Usuń**.
10. Kliknij **Utwórz**.

Dodawanie obciążeń do planów monitorowania

W zależności od potrzeb po utworzeniu planu monitorowania można do niego dodać obciążenia.

Wymagania wstępne

- Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.
- Wersja agenta zainstalowana na obciążeniu obsługuje funkcję monitorowania.
- Jest dostępny co najmniej jeden plan monitorowania.

Aby dodać obciążenie do planu monitorowania

W sekcji Plany monitorowania

1. W konsoli Ochrona przejdź do sekcji **Zarządzanie** > **Plany monitorowania**.
2. Kliknij plan monitorowania.
3. W zależności od tego, czy plan został już zastosowany do jakiegoś obciążenia, wykonaj następujące czynności:
   - Kliknij **Dodaj obciążenia**, jeśli plan nie został jeszcze zastosowany do żadnego obciążenia.
   - Jeśli plan nie został jeszcze zastosowany do żadnego obciążenia, kliknij **Zarządzaj obciążeniami**.
4. Wybierz obciążenie z listy i kliknij **Dodaj**.
5. Kliknij **Zapisz**.
6. W razie potrzeby kliknij **Potwierdź**, aby zastosować do obciążenia wymagany limit usługi.

W sekcji Wszystkie urządzenia

© Acronis International GmbH, 2003-2024

1. W konsoli Ochrona przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie, do którego chcesz zastosować plan monitorowania.
3. Kliknij **Chroń**.
4. Znajdź plan monitorowania, do którego chcesz dodać obciążenie, i kliknij **Zastosuj**.
5. W razie potrzeby kliknij **Potwierdź**, aby zastosować do obciążenia wymagany limit usługi.

Odwoływanie planów monitorowania

Plan monitorowania można odwołać z obciążenia, do którego został on zastosowany.

Wymagania wstępne

Do obciążenia zastosowano co najmniej jeden plan monitorowania.

Aby odwołać plan monitorowania

1. W konsoli Ochrona przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie, a następnie kliknij **Chroń**.
3. Kliknij ikonę **Więcej czynności** obok planu monitorowania, który chcesz odwołać, a następnie kliknij **Odwołaj**.

Konfigurowanie automatycznych czynności w ramach reagowania

Automatyczne czynności w ramach reagowania na zgłoszone za pomocą alertów zdarzenia to predefiniowane czynności lub środki, które są automatycznie wyzwalane w reakcji na wykryte zdarzenia lub incydenty. Czynności te mają na celu złagodzenie potencjalnych zagrożeń i zminimalizowanie szkód.

Można skonfigurować jedną lub kilka automatycznych czynności w ramach reagowania na zdarzenia zgłaszane za pomocą alertów. Można skonfigurować maksymalnie 20 automatycznych czynności w ramach reagowania na monitor.

Aby skonfigurować automatyczne czynności w ramach reagowania

1. W konsoli Ochrona przejdź do sekcji **Zarządzanie** > **Plany monitorowania**.
2. Wybierz plan monitorowania, dla którego chcesz skonfigurować automatyczne czynności w ramach reagowania.
3. Wybierz monitor, dla którego chcesz skonfigurować automatycznej czynności w ramach reagowania, a jeśli nie dodano jeszcze żadnego monitora, kliknij **Dodaj monitor**, kliknij monitor na liście, kliknij **Dodaj**, a następnie wybierz monitor.
4. Kliknij łącze widoczne obok pozycji **Automatyczne czynności w ramach reagowania**.
5. W oknie **Automatyczne czynności w ramach reagowania** dodaj co najmniej jedną czynność w ramach reagowania, która ma zostać automatycznie wykonana po wyzwoleniu alertu.
6. Skonfiguruj każdą czynność w ramach reagowania. Jeśli na przykład dodano czynność w ramach reagowania **Uruchom usługę systemu Windows**, wykonaj następujące czynności:

© Acronis International GmbH, 2003-2024

a. Następnie obok pozycji **Usługa systemu Windows** kliknij **Określ**.

b. W polu **Usługa** wybierz usługę, która ma zostać uruchomiona jako czynność w ramach reagowania.

c. Kliknij **Gotowe**.

7. Na liście wszystkich dodanych czynności w ramach reagowania użyj strzałki w górę i strzałki w dół lub przeciągnij pozycje, aby określić kolejność czynności w ramach reagowania.
8. Skonfiguruj sposób obsługi kolejnych czynności w ramach reagowania, jeśli poprzednia czynność się nie powiedzie. Wybierz jedną z następujących opcji:
   a. **Wykonaj następną czynność w ramach reagowania**.
   b. **Nie wykonuj następnej czynności w ramach reagowania**.
9. Kliknij **Gotowe**.

   Liczba skonfigurowanych czynności będzie wyświetlana obok ustawienia **Czynności w ramach reagowania** w planie monitorowania. Można te czynności edytować lub usuwać, a ponadto w każdej chwili można też dodawać nowe.

W poniższej tabeli zestawiono i opisano wszystkie automatyczne czynności w ramach reagowania dostępne w ustawieniach monitora.

Automatyczna czynność w ramach reagowania	Opis	Obsługiwany system operacyjny
Uruchom skrypt	Możliwości dostępne w przypadku dodania tej czynności: 1. Wybranie konkretnego skryptu do uruchomienia na obciążeniu. 2. Wskazanie konta, na którym ma zostać wykonany skrypt. 3. Określenie maksymalnego czasu trwania operacji. 4. Określenie zasad wykonywania w programie PowerShell. 5. Uruchomienie skryptu. Do wykonania tej czynności potrzebna jest licencja pakietu Zarządzanie zaawansowane dla obciążenia (jeśli nie została jeszcze przypisana). Gdy zostaną spełnione podane warunki, system uruchomi wybrany skrypt zdalny z określonymi parametrami.	Windows, macOS
Uruchom ponownie obciążenie	W przypadku dodania tej czynności system zdalnie uruchomi obciążenie ponownie,	Windows, macOS

© Acronis International GmbH, 2003-2024

Automatyczna czynność w ramach reagowania	Opis	Obsługiwany system operacyjny
	gdy zostaną spełnione podane warunki.	
Zatrzymaj proces	W przypadku dodania tej czynności można wskazać proces do zatrzymania przez ręczne wpisanie jego nazwy. System zatrzyma proces, gdy zostaną spełnione podane warunki.	Windows, macOS
Uruchom usługę systemu Windows	W przypadku dodania tej czynności można wybrać usługę systemu Windows do uruchomienia z dynamicznej listy usług wypełnianej na podstawie agentów. System uruchomi tę usługę, gdy zostaną spełnione podane warunki.	Windows
Zatrzymaj usługę systemu Windows	W przypadku dodania tej czynności można wybrać usługę systemu Windows do zatrzymania z dynamicznej listy usług wypełnianej na podstawie agentów. System zatrzyma tę usługę, gdy zostaną spełnione podane warunki.	Windows
Włącz usługę Windows Update	W przypadku dodania tej czynności system włączy usługę Windows Update, gdy zostaną spełnione podane warunki. Czynność ta jest dostępna tylko w przypadku monitora statusu usługi Windows Update.	Windows
Wyłącz funkcję uruchamiania automatycznego na dyskach wymiennych	W przypadku dodania tej czynności system wyłączy dla obciążenia funkcję uruchamiania automatycznego na wymiennych nośnikach pamięci, gdy zostaną spełnione podane warunki. Ta czynność jest dostępna tylko w przypadku monitora statusu funkcji uruchamiania automatycznego.	Windows

Dodatkowe czynności dotyczące planów monitorowania

Na ekranie **Plany monitorowania** możesz wykonywać następujące dodatkowe czynności związane z planami monitorowania: wyświetlanie szczegółów, edytowanie, wyświetlanie działań, wyświetlanie

© Acronis International GmbH, 2003-2024

alertów, zmienianie nazwy, włączanie, wyłączanie, klonowanie, eksportowanie, ustawianie jako ulubione, ustawianie jako domyślne i usuwanie.

Wyświetl szczegóły

Aby wyświetlić szczegóły planu monitorowania

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Wyświetl szczegóły**.
3. [Opcjonalnie] Jeśli zechcesz wyświetlić szczegóły monitora włączonego w planie, kliknij jego nazwę.

Edytuj

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby edytować plan

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Edytuj**.
3. [Opcjonalnie] Aby usunąć monitor z planu, kliknij ikonę kosza znajdującą się po prawej stronie nazwy monitora.
4. [Opcjonalnie] Aby włączyć lub wyłączyć monitor w planie, użyj przełącznika widocznego obok nazwy monitora.
5. [Opcjonalnie] Aby edytować parametry monitora, wykonaj następujące czynności.
   a. Kliknij nazwę monitora.
   b. Kliknij przegląd parametrów monitora.
   c. Na ekranie **Parametry monitora** skonfiguruj parametry, a następnie kliknij **Gotowe**.

      Uwaga
      W przypadku każdego monitora można skonfigurować inne ustawienia. Dodatkowe informacje można znaleźć w sekcjach "Konfigurowalne monitory" (s. 1121) i "Konfigurowanie alertów dotyczących monitorowania" (s. 1168).

   d. Zamknij ekran i potwierdź zmiany.
6. [Opcjonalnie] Aby dodać monitor, kliknij **Dodaj monitor**, a następnie, jeśli zajdzie taka potrzeba, edytuj parametry zgodnie z wyjaśnieniem podanym w poprzednim kroku.
7. Kliknij **Zapisz**.

Działania

Aby wyświetlić działania dotyczące planu monitorowania

© Acronis International GmbH, 2003-2024

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Działania**.
3. Kliknij działanie, aby wyświetlić więcej informacji na jego temat.

Alerty

Aby wyświetlić alerty

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Alerty**.

Zmień nazwę

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby zmienić nazwę planu monitorowania

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Zmień nazwę**.
3. Wprowadź nową nazwę planu, a następnie kliknij **OK**.

Włącz

Wymagania wstępne

- Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.
- Plan monitorowania został zastosowany do co najmniej jednego obciążenia.

Aby włączyć plan monitorowania

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Włącz**.

Wyłącz

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby wyłączyć plan monitorowania

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Wyłącz**.

© Acronis International GmbH, 2003-2024

Klonuj

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby sklonować plan monitorowania

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Klonuj**.
3. Kliknij **Utwórz**.

Eksportuj

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby wyeksportować plan monitorowania

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Eksportuj**.
   Konfiguracja planu zostanie wyeksportowana na komputer lokalny w formacie JSON.

Usuń

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby usunąć plan monitorowania

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Usuń**.
3. Wybierz **Potwierdzam**, a następnie kliknij **Usuń**.

Ustaw jako domyślne

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby ustawić plan monitorowania jako domyślny

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Ustaw jako domyślne**.

© Acronis International GmbH, 2003-2024

3. W oknie potwierdzenia kliknij **Ustaw**.
   Na ekranie **Plany monitorowania** obok nazwy planu będzie widoczny znacznik **Domyślne**.

Dodawanie do ulubionych

Wymagania wstępne

Dla Twojego konta użytkownika zostało włączone uwierzytelnianie dwuskładnikowe.

Aby ustawić plan monitorowania jako ulubiony

1. Na ekranie **Plany monitorowania** kliknij ikonę **Więcej czynności** widoczną obok wybranego planu monitorowania.
2. Kliknij **Dodaj do ulubionych**.
   Na ekranie **Plany monitorowania** obok nazwy planu będzie widoczna ikona gwiazdki.

Problemy z kompatybilnością dotyczące planów monitorowania

W niektórych przypadkach zastosowanie planu monitorowania na obciążeniu może spowodować problemy z kompatybilnością. Można zauważyć następujące problemy z kompatybilnością:

- Niekompatybilny system operacyjny — ten problem jest powodowany nieobsługiwanym systemem operacyjnym obciążenia.
- Nieobsługiwany agent — ten problem występuje, gdy na obciążeniu znajduje się agent ochrony w przestarzałej wersji, który nie obsługuje funkcji monitorowania.
- Za mały limit — ten problem występuje, gdy dzierżawca ma zbyt mały limit usługi, aby można było ją przypisać do wybranych obciążeń.

Jeśli plan monitorowania jest stosowany do maksymalnie 150 indywidualnie wybranych obciążeń, zostanie wyświetlony monit o rozwiązanie istniejących konfliktów przed zapisaniem planu. Aby rozwiązać konflikt, wyeliminuj jego główną przyczynę lub usuń z planu obciążenia, których dotyczy ten konflikt. Aby uzyskać więcej informacji, zobacz "Rozwiązywanie problemów z kompatybilnością dotyczących planów monitorowania" (s. 1166). W przypadku zapisania planu bez rozwiązania konfliktów zostanie on automatycznie wyłączony dla niekompatybilnych obciążeń i zostaną wyświetlone alerty.

Jeśli plan monitorowania jest stosowany do więcej niż 150 obciążeń lub do grup urządzeń, najpierw zostanie zapisany, a następnie sprawdzony pod kątem kompatybilności. Plan ten zostanie automatycznie wyłączony dla niekompatybilnych obciążeń i zostaną wyświetlone alerty.

Rozwiązywanie problemów z kompatybilnością dotyczących planów monitorowania

W zależności od przyczyny problemów z kompatybilnością można wykonać różne czynności w celu rozwiązania problemów z kompatybilnością w ramach procesu tworzenia nowego planu monitorowania.

Aby rozwiązać problemy z kompatybilnością

© Acronis International GmbH, 2003-2024

1. Kliknij **Przejrzyj problemy**.
2. [Opcjonalnie] Aby rozwiązać problemy z kompatybilnością spowodowane przez niekompatybilne systemy operacyjne, usuwając obciążenia z planu:
   a. Na karcie **Niekompatybilny system operacyjny** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
3. [Opcjonalnie] Aby rozwiązać problemy z kompatybilnością spowodowane przez niekompatybilne systemy operacyjne, wyłączając monitor w planie:
   a. Na karcie **Niekompatybilny system operacyjny** wybierz monitory do usunięcia.
   b. Kliknij **Wyłącz monitor**.
   c. Kliknij **Wyłącz**, a następnie kliknij **Zamknij**.
4. [Opcjonalnie] Aby rozwiązać problemy z kompatybilnością spowodowane przez nieobsługiwane agenty, usuwając obciążenia z planu:
   a. Na karcie **Nieobsługiwane agenty** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
5. [Opcjonalnie] Aby rozwiązać problemy z kompatybilnością spowodowane przez nieobsługiwane agenty, aktualizując wersje agentów, kliknij **Przejdź do listy agentów**.

   Uwaga
   Ta opcja jest dostępna wyłącznie dla administratorów klientów.

6. [Opcjonalnie] Aby rozwiązać problemy z kompatybilnością spowodowane przez za mały limit, usuwając obciążenia z planu:
   a. Na karcie **Za mały limit** wybierz obciążenia do usunięcia.
   b. Kliknij **Usuń obciążenia z planu**.
   c. Kliknij **Usuń**, a następnie **Zamknij**.
7. [Opcjonalnie] Aby rozwiązać problemy ze zgodnością spowodowane za małym limitem, zwiększając limit dzierżawcy:
   a. Na karcie **Za mały limit** kliknij **Przejdź do portalu zarządzania**.
   b. Zwiększ limit usługi dla klienta.

   Uwaga
   Ta opcja jest dostępna wyłącznie dla administratorów partnerów.

Resetowanie modeli uczenia maszynowego

Gdy modele obciążenia staną się nieaktualne bądź z jakiegoś powodu nieprawidłowe, możesz je zresetować. Ta czynność spowoduje usunięcie utworzonych modeli oraz danych dotyczących

© Acronis International GmbH, 2003-2024

obciążenia zebranych przez monitory obsługujące monitorowanie typu Wykrywanie anomalii, po czym szkolenie modeli uczenia maszynowego dla obciążenia rozpocznie się od początku.

Aby zresetować modele uczenia maszynowego dla obciążenia

1. W konsoli Ochrona przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie na liście, a następnie kliknij kartę **Szczegóły**.
3. W sekcji **Zresetuj modele uczenia maszynowego** kliknij opcję **Zresetuj**.
4. W oknie z monitem o potwierdzenie kliknij ponownie opcję **Zresetuj**.

Alerty dotyczące monitorowania

Alerty z monitorowania są wyświetlane w konsoli Ochrona i wysyłane za pośrednictwem poczty e-mail, gdy monitorowane zachowanie obciążenia jest niezgodne z normą. Alerty gwarantują jak najszybsze informowanie interesariuszy o wszelkich problemach w środowisku IT organizacji.

Uwaga
Aby włączyć alerty z monitorowania za pośrednictwem poczty e-mail, trzeba skonfigurować co najmniej jedną zasadę powiadomień e-mail dla odpowiedniego typu alertu. Aby uzyskać więcej informacji, zobacz "Konfigurowanie zasad powiadamiania pocztą e-mail" (s. 1176).

Konfigurowanie alertów dotyczących monitorowania

Ustawienia alertów monitora można skonfigurować podczas dodawania monitora do planu monitorowania lub podczas edytowania monitora, który jest już dostępny w planie monitorowania.

Aby skonfigurować alerty dotyczące monitorowania

1. W oknie **Parametry monitora** przejdź do sekcji **Generuj alerty**.
2. W polu **Istotność alertu** wybierz istotność odpowiadającą priorytetowi alertu.

Opcja	Opis
Krytyczne	Te alerty mają najwyższy priorytet i są związane z problemami o znaczeniu krytycznym z perspektywy działania obciążenia. Rozwiąż te problemy jak najszybciej.
Błąd	Alert o błędzie jest mniej istotny i wskazuje, że coś jest nie tak lub nie zachowuje się normalnie. Rozwiąż te problemy na czas, aby zapobiec wystąpieniu poważniejszych problemów.
Ostrzeżenie	Alert ostrzegawczy wskazuje, że wystąpiła sytuacja, o której warto wiedzieć, choć może ona jeszcze nie powodować problemu. Rozwiąż te problemy po rozwiązaniu problemów powodujących alerty krytyczne i alerty o błędach. To jest wartość domyślna.

© Acronis International GmbH, 2003-2024

Opcja	Opis
Informacja	Te alerty mają najniższy priorytet. Alert informacyjny nie oznacza problemu. Takie alerty dostarczają informacji o czynnościach związanych z monitorowanym obiektem.

3. W polu **Częstotliwość alertu** określ, jak często system powinien generować alert, gdy jest spełniony dany warunek.

Opcja	Opis
Raz do pomyślnego wyniku sprawdzenia	System wygeneruje alert jeden raz do czasu pomyślnego zakończenia operacji sprawdzania. To jest wartość domyślna.
Po X niepowodzeniach z rzędu	System wygeneruje alert po X kolejnych operacjach sprawdzania zakończonych niepowodzeniem, gdzie wartość X jest liczbą całkowitą.

4. W polu **Komunikat alertu** kliknij ikonę ołówka, aby edytować domyślny komunikat alertu, który ma być używany, gdy system wygeneruje alert. Można określić własny komunikat alertu zawierający zmienne. Dodatkowe informacje na temat zmiennych, których można użyć, można znaleźć w sekcji "Zmienne alertów dotyczących monitorowania" (s. 1169).

   Uwaga
   W przypadku niektórych monitorów można skonfigurować więcej niż jeden komunikat alertu.

5. Włącz **Automatyczne rozwiązanie alertu**, jeśli system ma automatycznie rozwiązać alert, gdy monitorowany wskaźnik wróci do normalnego stanu i zachowanie znów będzie normalne. Domyślnie to ustawienie jest włączone.

Zmienne alertów dotyczących monitorowania

Można skonfigurować różne zmienne w alertach dla różnych monitorów. Aby użyć zmiennej, należy ją ująć w nawiasy klamrowe: {{}}.

Poniższa tabela zawiera dodatkowe informacje na temat zmiennych w alertach.

Zmienna	Opis	Dostępność dla monitorów
plan_name	Nazwa zasad	Wszystkie monitory
monitor_name	Nazwa zasad podrzędnych w planie monitorowania	Wszystkie monitory
workload_ name	Nazwa obciążenia	Wszystkie monitory
threshold_	Konkretne warunki do monitorowania lub	Wszystkie monitory

© Acronis International GmbH, 2003-2024

Zmienna	Opis	Dostępność dla monitorów
value	progi wygenerowania alertu	obsługujące monitorowanie typu Wykrywanie progów.
threshold_unit	Jednostka powiązana z wartością progową. Na przykład %, MB lub mb/s.	Wszystkie monitory obsługujące monitorowanie typu Wykrywanie progów.
time_period	System wygeneruje alert o wykrytym problemie tylko wtedy, gdy wartość wskaźnika będzie poza normą przez określony czas.	Wszystkie monitory obsługujące monitorowanie typu Wykrywanie progów.
time_unit	Jednostka, która będzie powiązana z okresem (sekunda, minuta, godzina lub dzień).	Wszystkie monitory obsługujące monitorowanie typu Wykrywanie progów.
anomaly_value	Wartość oznaczająca anomalię	Wszystkie monitory obsługujące monitorowanie typu Wykrywanie anomalii.
anomaly_unit	Jednostka, która będzie powiązana z wartością oznaczającą anomalię	Wszystkie monitory obsługujące monitorowanie typu Wykrywanie anomalii.
deviation_value	Wartość wyznaczająca odchylenie	Wszystkie monitory obsługujące monitorowanie typu Wykrywanie anomalii.
deviation_unit	Jednostka, która będzie powiązana z wartością wyznaczającą odchylenie	Wszystkie monitory obsługujące monitorowanie typu Wykrywanie anomalii.
drive_name	Dysk w przypadku systemu Windows lub partycja w przypadku systemu macOS	Miejsce na dysku.
CPU_model	Model monitorowanego procesora	Temperatura procesora
GPU_model	Model monitorowanego procesora graficznego	Temperatura procesora graficznego
hardware_ model	Model monitorowanego komponentu	Zmiany sprzętowe
hardware_ component	Typ monitorowanego sprzętu	Zmiany sprzętowe
hardware_ model_old	Model monitorowanego wymienionego komponentu	Zmiany sprzętowe
hardware_	Model monitorowanego nowo dodanego	Zmiany sprzętowe

© Acronis International GmbH, 2003-2024

Zmienna	Opis	Dostępność dla monitorów
model_new	komponentu	
disk_model	Model dysku	Szybkość transferu dysku
network_ adapter_model	Model karty sieciowej	Wykorzystanie sieci
process_name	Nazwa procesu	Poziom użycia procesora przez proces Poziom użycia pamięci przez proces Szybkość transferu dysku generowanego przez proces Poziom użycia sieci przez proces Status procesu
service_name	Nazwa usługi	Status usług systemu Windows
software_name	Nazwa aplikacji	Zainstalowane oprogramowanie
software_ version	Wersja aplikacji	Zainstalowane oprogramowanie
software_ version_old	Wersja aplikacji przed aktualizacją	Zainstalowane oprogramowanie
software_ version_new	Wersja nowej lub zaktualizowanej aplikacji	Zainstalowane oprogramowanie
number_of_ occurrences	Liczba wystąpień zdarzenia w dzienniku	Dziennik zdarzeń systemu Windows
event_types	Typ zdarzenia	Dziennik zdarzeń systemu Windows
event_source	Źródło zdarzenia	Dziennik zdarzeń systemu Windows
event_log_ name	Nazwa zdarzenia	Dziennik zdarzeń systemu Windows
firewall_	Nazwa oprogramowania zapory	Status zapory

© Acronis International GmbH, 2003-2024

Zmienna	Opis	Dostępność dla monitorów
software_name		
antimalware_ software_name	Nazwa oprogramowania antywirusowego	Status oprogramowania antywirusowego
user_name	Nazwa użytkownika	Status funkcji uruchamiania automatycznego
script_name	Nazwa skryptu	Niestandardowe

Ręczne czynności w ramach reagowania

Po wyświetleniu alertu możesz wybrać czynność w ramach reagowania, która ma zostać wykonana w odniesieniu do zdarzeń zgłoszonych za pomocą alertu.

Aby wykonać ręczną czynność w ramach reagowania

1. W konsoli Ochrona przejdź do sekcji **Alerty**.
2. Otwórz alert, który chcesz wyświetlić.
3. Kliknij **Czynność w ramach reagowania**, a następnie wybierz jedną z czynności widocznych na liście rozwijanej.

Lista czynności w ramach reagowania dostępnych w przypadku danego alertu zależy od typu alertu, dostępności funkcji dla danego dzierżawcy i systemu operacyjnego obciążenia.

Poniższa tabela zawiera listę i opisy wszystkich ręcznych czynności w ramach reagowania.

Ręczna czynność w ramach reagowania	Opis	Obsługiwany system operacyjny
Przeglądaj trend wykorzystania miejsca na dysku	Powoduje otwarcie okna z wykresem **Wykorzystanie miejsca na dysku**, który umożliwia: • Przeglądanie zmian wykorzystania miejsca na dysku w czasie (w ciągu ostatniego okresu: 1 dzień / 7 dni / 1 miesiąc). • Przeglądanie zmian wykorzystania miejsca na dysku w wartości względnej (%) w ramach wybranego okresu.	Windows, macOS
Przeglądaj trend wzrostu rozmiaru plików	Powoduje otwarcie okna z wykresem **Wzrost rozmiaru plików**, który umożliwia:	Windows, macOS

© Acronis International GmbH, 2003-2024

Ręczna czynność w ramach reagowania	Opis	Obsługiwany system operacyjny
	• Przeglądanie zmian łącznego rozmiaru monitorowanych plików i folderów w czasie (w ciągu ostatniego okresu: 1 dzień / 7 dni / 1 miesiąc). • Przeglądanie zmian łącznego rozmiaru plików w wartości względnej (%) w ramach wybranego okresu.	
Uruchom skrypt	Powoduje otwarcie okna, które umożliwia: 1. Wybranie konkretnego skryptu do uruchomienia na obciążeniu. 2. Wskazanie konta, na którym ma zostać wykonany skrypt. 3. Określenie maksymalnego czasu trwania operacji. 4. Określenie zasad wykonywania w programie PowerShell. 5. Uruchomienie skryptu. Do wykonania tej czynności potrzebna jest licencja pakietu Zarządzanie zaawansowane dla obciążenia (jeśli nie została jeszcze przypisana).	Windows, macOS
Połącz przy użyciu protokołu NEAR	Acronis Klient rozwiązania Connect nawiązuje połączenie zdalne.	Windows, macOS
Połącz przy użyciu protokołu RDP	Acronis Klient rozwiązania Connect nawiązuje połączenie zdalne.	Windows
Otwórz inwentaryzację sprzętu	Nastąpi przekierowanie do karty **Inwentaryzacja sprzętu** dla bieżącego obciążenia.	Windows, macOS
Przeglądaj 10 procesów najbardziej obciążających procesor	Powoduje otwarcie okna z 10 procesami, które najbardziej obciążają procesor, w związku z czym mogą powodować jego przegrzanie (migawka systemu w chwili wygenerowania alertu).	Windows, macOS
Przeglądaj 10 procesów najbardziej obciążających procesor graficzny	Powoduje otwarcie okna z 10 procesami, które najbardziej obciążają procesor graficzny, w związku z czym mogą powodować jego przegrzanie (migawka systemu w chwili wygenerowania alertu).	Windows, macOS

© Acronis International GmbH, 2003-2024

Ręczna czynność w ramach reagowania	Opis	Obsługiwany system operacyjny
Przeglądaj 10 procesów najbardziej obciążających pamięć	Powoduje otwarcie okna z 10 procesami, które najbardziej obciążają pamięć operacyjną (migawka systemu w chwili wygenerowania alertu).	Windows, macOS
Przeglądaj 10 procesów najbardziej obciążających dysk	Powoduje otwarcie okna z 10 procesami, które najbardziej obciążają dysk (migawka systemu w chwili wygenerowania alertu).	Windows, macOS
Przeglądaj 10 procesów najbardziej obciążających sieć	Powoduje otwarcie okna z 10 procesami, które najbardziej obciążają kartę sieciową (migawka systemu w chwili wygenerowania alertu).	Windows, macOS
Przeglądaj użycie zasobów przez proces	Powoduje otwarcie okna ze szczegółowymi informacjami o wykorzystaniu zasobów sprzętowych przez powiązany proces: użycie procesora, użycie pamięci, we/wy dysku, wykorzystanie sieci.	Windows, macOS
Uruchom ponownie obciążenie	Powoduje otwarcie okna potwierdzenia. Po potwierdzeniu obciążenie zostaje uruchomione ponownie.	Windows, macOS
Uruchom usługę systemu Windows	Powoduje otwarcie okna potwierdzenia. Po potwierdzeniu uruchamia usługę systemu Windows.	Windows
Zatrzymaj usługę systemu Windows	Powoduje otwarcie okna potwierdzenia. Po potwierdzeniu zatrzymuje usługę systemu Windows.	Windows
Zatrzymaj proces	Powoduje otwarcie okna potwierdzenia. Po potwierdzeniu zatrzymuje proces, do którego odnosi się alert.	Windows, macOS
Włącz usługę Windows Update	Powoduje otwarcie okna potwierdzenia. Po potwierdzeniu włącza usługę Windows Update.	Windows
Wyłącz funkcję uruchamiania automatycznego na dyskach wymiennych	Powoduje otwarcie okna potwierdzenia. Po potwierdzeniu wyłącza na obciążeniu funkcję uruchamiania automatycznego na poziomie systemu.	Windows

© Acronis International GmbH, 2003-2024

Ważne
Ze względów bezpieczeństwa trzeba skorzystać z uwierzytelniania dwuskładnikowego w celu wykonania następujących ręcznych czynności w ramach reagowania:

- Uruchom skrypt
- Połącz przy użyciu protokołu NEAR
- Połącz przy użyciu protokołu RDP
- Uruchom ponownie obciążenie
- Uruchom usługę systemu Windows
- Zatrzymaj usługę systemu Windows
- Zatrzymaj proces
- Włącz usługę Windows Update
- Wyłącz funkcję uruchamiania automatycznego na dyskach wymiennych

Wyświetlanie alertów z monitorowania dotyczących wybranego obciążenia

Na karcie **Alerty** można przeglądać alerty z monitorowania określonego obciążenia i wykonywać różne czynności związane z tym alertem.

Aby wyświetlić alerty z monitorowania dotyczące wybranego obciążenia

1. W konsoli Ochrona przejdź do sekcji **Wszystkie urządzenia**.
2. Kliknij obciążenie, a następnie wybierz kartę **Alerty**.
3. [Opcjonalnie] W panelu alertów z monitorowania wykonaj jedną z następujących czynności:
   - Aby wyczyścić alert, kliknij **Wyczyść**.
   - Aby została wykonana czynność w ramach reagowania, kliknij **Czynność w ramach reagowania**, a następnie kliknij czynność.
   - Aby skontaktować się z działem pomocy technicznej, kliknij **Uzyskaj pomoc**.
4. [Opcjonalnie] Aby wyczyścić wszystkie alerty z monitorowania dotyczące danego obciążenia, kliknij **Wyczyść wszystko**.

Wyświetlanie dziennika alertów dotyczących monitorowania

Możesz wyświetlić wszystkie zdarzenia związane z alertem dotyczącym monitorowania w kolejności chronologicznej: wykonane czynności w ramach reagowania (zarówno automatyczne, jak i ręczne) oraz wysłane powiadomienia e-mail.

Aby wyświetlić dziennik inspekcji alertu dotyczącego monitorowania

© Acronis International GmbH, 2003-2024

1. W konsoli Ochrona przejdź do sekcji **Alerty**.
2. Otwórz **Widok tabeli**.
3. Na liście alertów kliknij alert dotyczący monitorowania, który chcesz wyświetlić.
4. Kliknij **Szczegóły**, a następnie kliknij **Dziennik alertów**.

Konfigurowanie zasad powiadamiania pocztą e-mail

Zasady powiadamiania pocztą e-mail umożliwiają określenie, którzy użytkownicy mają otrzymywać powiadomienia e-mail od różnych monitorów.

Na ekranie **Powiadomienia e-mail** można wykonywać następujące czynności w odniesieniu do zasad powiadamiania pocztą e-mail: dodawanie, edycja, włączanie, wyłączanie i usuwanie.

Dodaj

Aby dodać nowe zasady powiadomień e-mail

1. W konsoli Ochrona przejdź do sekcji **Ustawienia** > **Powiadomienia e-mail**.
2. Kliknij **Dodaj zasady**.
3. Kliknij **Wybierz odbiorców**.
4. Na ekranie **Wybierz odbiorców** wybierz użytkowników, którzy mają otrzymywać alerty e-mail, a następnie kliknij **Wybierz**.
5. W oknie **Typy alertów** wybierz monitory, w których przypadku system ma wysyłać alerty e-mail.
6. Kliknij **Dodaj**.

Edytuj

Aby edytować zasady powiadomień e-mail

1. W konsoli Ochrona przejdź do sekcji **Ustawienia** > **Powiadomienia e-mail**.
2. Kliknij ikonę wielokropka zasad powiadomień, a następnie kliknij **Edytuj**.
3. [Opcjonalnie] Aby zmienić odbiorców, kliknij **Edytuj odbiorców**, dodaj lub usuń użytkowników na liście, a następnie kliknij **Wybierz**.
4. [Opcjonalnie] W sekcji **Typy alertów** wybierz typy alertów z monitorowania, które chcesz wysłać do wybranych odbiorców.
5. Kliknij **Zapisz**.

Włącz

Aby włączyć zasady powiadomień e-mail

1. W konsoli Ochrona przejdź do sekcji **Ustawienia** > **Powiadomienia e-mail**.
2. Na ekranie **Powiadomienia e-mail** kliknij ikonę **...** zasad powiadomień e-mail.
3. Kliknij **Włącz**.

Wyłącz

© Acronis International GmbH, 2003-2024

Aby wyłączyć zasady powiadomień e-mail

1. W konsoli Ochrona przejdź do sekcji **Ustawienia** > **Powiadomienia e-mail**.
2. Na ekranie **Powiadomienia e-mail** kliknij ikonę **...** zasad powiadomień e-mail.
3. Kliknij **Wyłącz**.

Usuń

Aby usunąć zasady powiadomień e-mail

1. W konsoli Ochrona przejdź do sekcji **Ustawienia** > **Powiadomienia e-mail**.
2. Na ekranie **Powiadomienia e-mail** kliknij ikonę **...** zasad powiadomień e-mail.
3. Kliknij **Usuń**, a następnie kliknij **Potwierdź**.

Wyświetlanie danych z monitora

W przypadku każdego obciążenia możesz wyświetlić listę zastosowanych monitorów, bieżący status monitorów oraz historyczne dane dotyczące wydajności w widoku graficznym. Możesz używać tych informacji do analizy stanu obciążenia oraz zmian tego stanu w czasie.

Wymagania wstępne

- Do obciążenia zastosowano plan monitorowania.
- Obciążenie jest w trybie online i zawiera dane dla odpowiedniego monitora.
- Wersja agenta zainstalowana na obciążeniu obsługuje plany monitorowania.

Aby wyświetlić monitory zastosowane do obciążenia i dane monitorów

1. W konsoli Ochrona przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij obciążenie, a następnie kliknij kartę **Monitorowanie**.
   Na karcie **Monitorowanie** zostanie wyświetlony widżet dla każdego monitora włączonego w przypadku danego obciążenia. Na każdym widżecie wyświetlane są następujące informacje.

Wyświetlana informacja	Opis
Nazwa monitora	Nazwa monitora
Ostatni wynik	Najnowsza wartość monitorowanego wskaźnika lub najnowszy stan zdarzenia
Ostatnie sprawdzenie	Data i godzina ostatniego zebrania danych przez monitor
Alerty	Liczba alertów, które zostały wygenerowane przez monitor, a nadal nie są obsłużone.

© Acronis International GmbH, 2003-2024

Wyświetlana informacja	Opis
	Jeśli monitor wygenerował przynajmniej jeden nieobsłużony alert, kliknięcie numeru spowoduje otwarcie karty **Alerty**. Alerty zostaną przefiltrowane i na liście będą widoczne tylko alerty związane z tym monitorem.

Uwaga
Widżety będą widoczne na karcie po 15 minutach od zastosowania planu monitorowania do obciążenia (lub z minimalną częstotliwością ustawioną dla monitora).

3. [Opcjonalnie] Aby wyświetlić więcej szczegółów na temat monitora i — w stosownych przypadkach — dane historyczne zebrane w przypadku monitorowanego wskaźnika, na widżecie monitora kliknij ikonę wielokropka, a następnie kliknij **Szczegóły**.

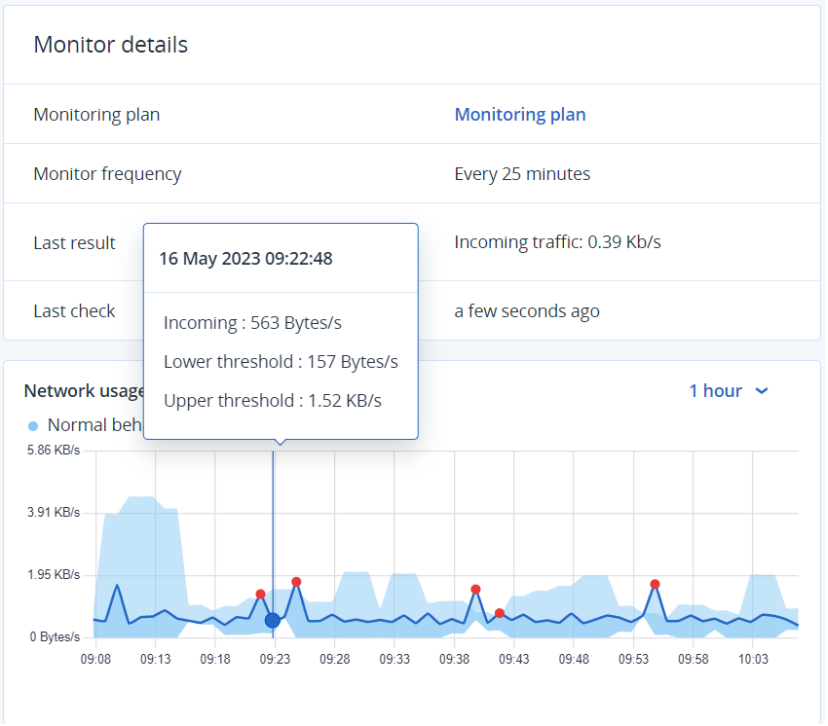
   Dodatkowe informacje na temat szczegółów monitora widocznych na widżetach można znaleźć w sekcji "Widżety monitorów" (s. 1178).

Widżety monitorów

Na widżecie monitora są widoczne następujące szczegóły dotyczące monitora.

Szczegół	Opis
Plan monitorowania	Nazwa planu monitorowania zawierającego monitor. Nazwa planu monitorowania jest łączem, które umożliwia otwarcie planu monitorowania w trybie widoku.
Częstotliwość monitorowania	Przedział czasu, w którym monitor zbiera dane z obciążenia
Ostatni wynik	Najnowsza wartość monitorowanego wskaźnika lub najnowszy stan zdarzenia
Ostatnie sprawdzenie	Data i godzina ostatniego zebrania danych przez monitor
Ostatni alert	Data i godzina wygenerowania ostatniego alertu. To pole jest wyświetlane tylko wtedy, gdy w przypadku monitora został wygenerowany co najmniej jeden alert.
Wykres historyczny	W przypadku monitorów zbierających dane w seriach czasowych na widżecie są wyświetlane dane historyczne dla wybranego okresu (1 godzina, 6 godzin, 12 godzin, 1 dzień, 1 tydzień lub 1 miesiąc) w widoku graficznym. Na wykresie są wyświetlane rzeczywiste wartości wskaźników w wybranym okresie. Jeśli z jakiegoś powodu agent nie wysłał zebranych danych do chmury, brakujące wartości zostaną wyświetlone jako linia

© Acronis International GmbH, 2003-2024

Szczegół	Opis
	przerywana łącząca punkty danych z rzeczywistymi wartościami: tą, która poprzedza brakującą wartość, i tą, która po niej następuje. W przypadku monitorów korzystających z monitorowania typu **Wykrywanie anomalii** na wykresie wyświetlany jest obszar linii bazowej oraz linia pokazująca rzeczywiste wartości wskaźnika i anomalie. Anomalie to skoki, czyli wartości wykraczające poza linie bazowe, i są wyświetlane na wykresie jako czerwone punkty. Po wskazaniu wykresu myszą będzie widoczna rzeczywista wartość i wartości progów dotyczące określonego czasu.  **Uwaga** Dane na wykresie są wyświetlane w strefie czasowej systemu lokalnego. Jest to strefa czasowa przeglądarki obciążenia, z którego uzyskuje się dostęp do konsoli Ochrona.

© Acronis International GmbH, 2003-2024

Dodatkowe narzędzia Cyber Protection

Tryb zgodności

Tryb zgodności jest przeznaczony dla klientów o wyższych wymaganiach w zakresie ochrony. Tryb ten wymaga szyfrowania wszystkich kopii zapasowych i umożliwia jedynie lokalnie ustawiane hasła szyfrowania.

W trybie zgodności wszystkie kopie zapasowe utworzone w ramach dzierżawcy-klienta i jego jednostek są automatycznie szyfrowane algorytmem AES z kluczem 256-bitowym. Użytkownicy mogą ustawiać hasła szyfrowania tylko na chronionych urządzeniach — nie mogą ich ustawiać w planach ochrony.

Ważne
Trybu zgodności nie można wyłączyć.

Ograniczenia

- Tryb zgodności jest kompatybilny tylko z agentami w wersji 15.0.26390 lub nowszej.
- Tryb zgodności nie jest dostępny w przypadku urządzeń z systemami Red Hat Enterprise Linux 4.x i 5.x oraz ich pochodnymi.
- Usługi chmurowe nie mają dostępu do haseł szyfrowania. Ze względu na te ograniczenia w trybie zgodności dzierżawcy nie mają dostępu do niektórych funkcji.

Nieobsługiwane funkcje

W trybie zgodności dzierżawcy nie mają dostępu do następujących funkcji:

- Odzyskiwanie przy użyciu konsoli Cyber Protect
- Przeglądanie kopii zapasowych na poziomie plików przy użyciu konsoli Cyber Protect
- Kopia zapasowa z chmury do chmury
- Kopia zapasowa witryny internetowej
- Kopia zapasowa aplikacji
- Kopia zapasowa urządzeń mobilnych
- Skanowanie antywirusowe kopii zapasowych
- Bezpieczne odzyskiwanie
- Automatyczne tworzenie firmowych białych list
- Mapa ochrony danych
- Odzyskiwanie po awarii
- Raporty i pulpity nawigacyjne związane z niedostępnymi funkcjami

© Acronis International GmbH, 2003-2024

Ustawianie hasła szyfrowania

Hasło lokalnie trzeba ustawić lokalnie — na chronionym urządzeniu. Nie można ustawić hasła szyfrowania w planie ochrony. Bez hasła operacje tworzenia kopii zapasowej będą się kończyć niepowodzeniem.

Ostrzeżenie!
W przypadku zgubienia lub zapomnienia hasła nie da się odzyskać zaszyfrowanych kopii zapasowych.

Hasło szyfrowania można ustawić następująco:

1. Podczas instalacji agenta ochrony (dla systemu Windows, macOS i Linux).
2. Przy użyciu wiersza polecenia (w systemie Windows i Linux).
   Jest to jedyny sposób, aby ustawić hasło szyfrowania na urządzeniu wirtualnym.
   Więcej informacji o ustawianiu hasła szyfrowania za pomocą narzędzia **Acropsh** można znaleźć w sekcji "Szyfrowanie" (s. 474).
3. W aplikacji Cyber Protect Monitor (w systemie Windows i macOS).

Aby ustawić hasło szyfrowania w aplikacji Cyber Protect Monitor

1. Zaloguj się jako administrator na chronionym urządzeniu.
2. Kliknij ikonę narzędzia Cyber Protect Monitor w obszarze powiadomień (w systemie Windows) lub na pasku menu (w systemie macOS).
3. Kliknij ikonę koła zębatego.
4. Kliknij **Szyfrowanie**.
5. Ustaw hasło szyfrowania.
6. Kliknij **OK**.

Zmienianie hasła szyfrowania

Hasło szyfrowania można zmienić, dopóki plan ochrony nie utworzy jakichkolwiek kopii zapasowych.

Lepiej nie zmieniać hasła szyfrowania po utworzeniu kopii zapasowych, bo poskutkuje to niepowodzeniem kolejnych operacji tworzenia kopii zapasowych. Aby nadal chronić dany komputer, trzeba utworzyć dla niego nowy plan ochrony. Zmiana zarówno hasła szyfrowania, jak i planu ochrony spowoduje, że nowe kopie zapasowe będą szyfrowane przy użyciu zmienionego hasła. Nie wpłynie to na kopie zapasowe utworzone przed wprowadzeniem tych zmian.

Można też zachować zastosowany plan ochrony i tylko zmienić w nim nazwę pliku kopii zapasowej. Również w tym przypadku nowe kopie zapasowe będą szyfrowane przy użyciu zmienionego hasła. Więcej informacji o nazwie pliku kopii zapasowej można znaleźć w sekcji "Nazwa pliku kopii zapasowej" (s. 483).

Hasło szyfrowania można zmienić następująco:

© Acronis International GmbH, 2003-2024

1. W aplikacji Cyber Protect Monitor (w systemie Windows i macOS).
2. Przy użyciu wiersza polecenia (w systemie Windows i Linux).
   Więcej informacji o ustawianiu hasła szyfrowania za pomocą narzędzia **Acropsh** można znaleźć w sekcji "Szyfrowanie" (s. 474).

Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności

W trybie zgodności nie można odzyskiwać kopii zapasowych w konsoli Cyber Protect.

Dostępne są następujące opcje:

- Odzyskanie całego komputera, jego dysków lub plików przy użyciu nośnika startowego.
- Wyodrębnienie plików — za pomocą Eksploratora plików systemu Windows — z lokalnych kopii zapasowych komputerów z systemem Windows z zainstalowanym agentem.

Niezmienny magazyn

Korzystając z niezmiennego magazynu, można uzyskiwać dostęp do usuniętych kopii zapasowych w ustawionym okresie przechowywania. Można odzyskiwać zawartość z tych kopii zapasowych, ale nie można ich zmieniać, przenosić ani usuwać. Po zakończeniu okresu przechowywania usunięte kopie zapasowe zostaną trwale usunięte.

Niezmienny magazyn zawiera następujące kopie zapasowe:

- Kopie zapasowe usunięte ręcznie.
- Kopie zapasowe usunięte automatycznie zgodnie z ustawieniami określonymi w sekcji **Okres przechowywania** w planie ochrony lub w sekcji **Reguły przechowywania** w planie czyszczenia.

Usunięte kopie zapasowe nadal zajmują miejsce w niezmiennym magazynie i są za nie naliczane odpowiednie opłaty.

Usunięci dzierżawcy nie są obciążani żadnymi opłatami za magazyny, w tym za niezmienny magazyn.

Tryby niezmiennego magazynu

W przypadku dzierżawców-klientów niezmienny magazyn jest dostępny w następujących trybach:

Niezmienny magazyn jest dostępny w następujących trybach:

- **Tryb nadzoru**
  Możesz wyłączyć i ponownie włączyć niezmienny magazyn. Możesz zmienić okres przechowywania lub przejść do trybu zgodności.
- **Tryb zgodności**

Ostrzeżenie!
Wybranie trybu zgodności jest nieodwracalne.

© Acronis International GmbH, 2003-2024

Nie można wyłączyć niezmiennego magazynu. Nie można zmienić okresu przechowywania ani wrócić do trybu nadzoru.

Obsługiwane magazyny i agenty

- Niezmienny magazyn jest obsługiwany tylko w chmurze.

  Niezmienny magazyn jest dostępny w przypadku chmur hostowanych przez firmę Acronis oraz partnerów korzystających z rozwiązania Acronis Cyber Infrastructure w wersji 4.7.1 lub nowszej.

  Obsługiwane są wszystkie magazyny, których można używać razem z rozwiązaniem AcronisCyber Infrastructure Backup Gateway. Na przykład, magazyny Acronis Cyber Infrastructure, Amazon S3 i EC2 oraz Microsoft Azure.

  Niezmienny magazyn wymaga, aby port TCP 40440 był otwarty dla usługi Backup Gateway w infrastrukturze Acronis Cyber Infrastructure. W wersji 4.7.1 lub nowszej port TCP 40440 jest automatycznie otwierany w przypadku ruchu **publicznego typu Backup (ABGW)**. Dodatkowe informacje na temat typów ruchu można znaleźć w dokumentacji infrastruktury Acronis Cyber Infrastructure.
- Niezmienny magazyn wymaga agenta ochrony w wersji 21.12 (kompilacja 15.0.28532) lub nowszej.
- Obsługiwane są tylko kopie zapasowe w formacie TIBX (Wersja 12).

Włączanie niezmiennego magazynu

Ustawienia niezmiennego magazynu można konfigurować w konsoli Cyber Protect lub portalu zarządzania. W obu miejscach są dostępne te same ustawienia. W ramach poniższej procedury wykorzystano konsolę Cyber Protect. Informacje na temat konfigurowania ustawień niezmiennego magazynu w portalu zarządzania można znaleźć w sekcji Konfigurowanie niezmiennego magazynu w podręczniku administratora.

Konfiguracja ustawień niezmiennego magazynu jest możliwa tylko wtedy, gdy w ramach dzierżawcy, do którego należy konto administratora, jest włączone uwierzytelnianie dwuskładnikowe.

Aby włączyć niezmienny magazyn

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. Przejdź do sekcji **Ustawienia** > **Ustawienia systemu**.
3. Przewiń listę domyślnych opcji kopii zapasowych, a następnie kliknij **Niezmienny magazyn**.
4. Włącz przełącznik **Niezmienny magazyn**.
5. Określ okres przechowywania wynoszący od 14 do 3650 dni.

   Domyślny okres przechowywania to 14 dni. Dłuższy okres przechowywania danych poskutkuje zajęciem większej ilości miejsca w magazynie.
6. Wybierz tryb niezmiennego magazynu, a następnie potwierdź wybór, jeśli zostanie wyświetlony monit.

© Acronis International GmbH, 2003-2024

W trybie nadzoru można włączyć lub wyłączyć niezmienny magazyn oraz zmienić okres przechowywania. Można też zmienić tryb nadzoru na tryb zgodności.

Ostrzeżenie!
Przejście na tryb zgodności jest nieodwracalne. Po wybraniu trybu zgodności nie można wyłączyć niezmiennego magazynu. Nie można też zmienić jego trybu ani okresu przechowywania.

7. Kliknij **Zapisz**.
8. Aby istniejące już archiwum obsługiwało niezmienny magazyn, należy utworzyć w nim nową kopię zapasową.
   Aby utworzyć nową kopię zapasową, uruchom plan ochrony ręcznie lub zgodnie z harmonogramem.

Ostrzeżenie!
W przypadku usunięcia kopii zapasowej przed utworzeniem archiwum obsługującego niezmienny magazyn kopia zapasowa zostanie trwale usunięta.

Wyłączanie niezmiennego magazynu

Uwaga
Niezmienny magazyn można wyłączyć tylko w trybie nadzoru.

Aby wyłączyć niezmienny magazyn

1. Zaloguj się w konsoli Cyber Protect jako administrator.
2. W menu nawigacyjnym kliknij **Ustawienia** > **Ustawienia systemu**.
3. Przewiń listę domyślnych opcji kopii zapasowych, a następnie kliknij **Niezmienny magazyn**.
4. Wyłącz przełącznik **Niezmienny magazyn**.
5. Potwierdź wybór, klikając **Wyłącz**.

Ostrzeżenie!
Wyłączenie niezmiennego magazynu nie działa od razu. W okresie prolongaty wynoszącym 14 dni niezmienny magazyn jest nadal aktywny i można uzyskać dostęp do usuniętych kopii zapasowych zgodnie z ich pierwotnym okresem przechowywania. Po zakończeniu okresu prolongaty wszystkie kopie zapasowe przechowywane w niezmiennym magazynie zostaną nieodwracalnie usunięte.

Uzyskiwanie dostępu do usuniętych kopii zapasowych w niezmiennym magazynie

W ustawionym okresie przechowywania można uzyskiwać dostęp do usuniętych kopii zapasowych i odzyskiwać z nich dane.

© Acronis International GmbH, 2003-2024

Uwaga
Aby można było uzyskiwać dostęp do usuniętych kopii zapasowych, dopilnuj, aby magazyn kopii zapasowych miał włączony port 40440 dla połączeń przychodzących.

Aby uzyskać dostęp do usuniętej kopii zapasowej

1. Na karcie **Magazyn kopii zapasowych** wybierz chmurę zawierającą usuniętą kopię zapasową.
2. [Tylko w przypadku usuniętych archiwów] Aby wyświetlić usunięte archiwa, kliknij **Pokaż usunięte**.
3. Wybierz archiwum zawierające kopię zapasową, którą chcesz odzyskać.
4. Kliknij **Pokaż kopie zapasowe**, a następnie **Pokaż usunięte**.
5. Wybierz kopię zapasową do odzyskania.
6. Przejdź do odzyskiwania zgodnie z opisem podanym w sekcji "Odzyskiwanie" (s. 532).

Magazyn z geograficzną nadmiarowością

Magazyn z geograficzną nadmiarowością zapewnia trwałość danych przez ich asynchroniczne kopiowanie do lokalizacji dodatkowej, geograficznie oddalonej od lokalizacji podstawowej. Geograficzna nadmiarowość sprawia, że dane są dostępne nawet wtedy, gdy lokalizacja podstawowa jest niedostępna.

Ważne
Zreplikowane dane zajmują tyle samo miejsca w pamięci masowej co dane oryginalne.

Włączanie i wyłączanie magazynu z geograficzną nadmiarowością

Wymagania wstępne

- Magazyn z geograficzną nadmiarowością będzie dostępny w konsoli Cyber Protect dopiero wtedy, gdy administrator partnera włączy go w Portalu zarządzania lub za pośrednictwem interfejsu API.
- Tylko administratorzy mogą włączać lub wyłączać magazyn z geograficzną nadmiarowością w konsoli Cyber Protect. Upewnij się, że masz uprawnienia administratora.

Aby włączyć magazyn z geograficzną nadmiarowością

1. [Tylko jeśli magazyn z geograficzną nadmiarowością został włączony za pośrednictwem interfejsu API] W alercie u góry o treści „Nadmiarowość geograficzna jest dostępna w przypadku wszystkich danych w chmurze” kliknij **Włącz Geo-redundant Cloud Storage**.
2. W konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Ustawienia systemu**.
3. Przewiń listę domyślnych opcji kopii zapasowych, a następnie kliknij **Geo-redundant Cloud Storage**.
4. Włącz przełącznik **Geo-redundant Cloud Storage**.
5. Kliknij **Zapisz**.

© Acronis International GmbH, 2003-2024

Teraz dane będą replikowane do lokalizacji dodatkowej i pozostaną dostępne nawet w przypadku awarii lokalizacji podstawowej.

Aby wyłączyć magazyn z geograficzną nadmiarowością

Ostrzeżenie!
Zreplikowane dane są usuwane w ciągu jednego dnia po wyłączeniu geograficznej nadmiarowości.

1. W konsoli Cyber Protect przejdź do sekcji **Ustawienia** > **Ustawienia systemu**.
2. Przewiń listę opcji kopii zapasowych, a następnie kliknij **Geo-redundant Cloud Storage**.
3. Wyłącz przełącznik **Geo-redundant Cloud Storage**.
4. Potwierdź wybór, wpisując **Wyłącz**, a następnie kliknij **Wyłącz**.

Status georeplikacji

Geograficzna nadmiarowość oznacza, że dane są replikowane do lokalizacji dodatkowej. Status georeplikacji wskazuje etapy tego procesu. Możliwe są następujące statusy:

- **Zsynchronizowano** — dane zostały zreplikowane do lokalizacji dodatkowej.
- **Synchronizowanie** — dane właśnie są replikowane do lokalizacji dodatkowej. Czas trwania tej operacji zależy od rozmiaru danych.
- **Wstrzymano** — replikacja danych została tymczasowo zawieszona.
- **Wyłączono** — replikacja danych została wyłączona.

Aby sprawdzić status replikacji w konsoli Cyber Protect

1. W konsoli Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych**.
2. Wybierz lokalizację, a następnie zestaw kopii zapasowych.
3. Kliknij **Szczegóły**, a następnie sprawdź status w polu **Status georeplikacji**.

Ograniczenia

- Obecnie lokalizacje dodatkowe na potrzeby replikowanych danych są dostępne tylko w Stanach Zjednoczonych, Niemczech i Kanadzie.
- Informacje na temat ograniczeń usługi Odzyskiwanie po awarii w przypadku korzystania z geograficznej nadmiarowości można znaleźć w dokumentacji usługi Odzyskiwanie po awarii.

© Acronis International GmbH, 2003-2024

Słownik

A

Agent ochrony

Agent ochrony to agent przeznaczony do instalowania na komputerach w celu zapewnienia ochrony danych.

Agent ochrony przed utratą danych

Komponent kliencki systemu ochrony przed utratą danych, który chroni hosta przed nieuprawnionym wykorzystywaniem, przesyłaniem i przechowywaniem poufnych, chronionych lub wrażliwych danych dzięki zastosowaniu kombinacji technik analizy kontekstu i zawartości oraz egzekwowanie centralnie zarządzanych zasad ochrony przed utratą danych. Rozwiązanie Cyber Protection udostępnia w pełni funkcjonalnego agenta ochrony przed utratą danych. Funkcjonalność tego agenta na chronionym komputerze jest jednak ograniczona do zestawu funkcji ochrony przed utratą danych dostępnych na potrzeby licencjonowania rozwiązania Cyber Protection i zależy od planu ochrony zastosowanego do tego komputera.

B

Baza danych urządzeń USB

[Kontrola urządzeń] Moduł kontroli urządzeń prowadzi bazę danych urządzeń USB, z której można je dodawać do listy wykluczeń z kontroli dostępu do urządzeń. Baza danych rejestruje urządzenia USB przy użyciu ich identyfikatorów, które można wprowadzać ręcznie lub wybierać spośród znanych urządzeń w konsoli Cyber Protect.

Brama VPN (dawniej nazywana serwerem VPN lub bramą łączności)

[Disaster Recovery] Specjalna maszyna wirtualna zapewniająca połączenie między lokalizacją lokalną a lokalizacją w chmurze przez bezpieczny tunel VPN. Brama VPN jest wdrażana w lokalizacji w chmurze.

D

Docelowy punkt odzyskiwania (RPO)

[Odzyskiwanie po awarii] Ilość danych utraconych w wyniku przestoju mierzona ilością czasu, który upłynął od zaplanowanego przestoju lub awarii. Próg RPO określa maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania nadającym się do wykorzystania w celu przełączenia awaryjnego a czasem bieżącym.

F

Finalizacja

Operacja zmiany tymczasowej maszyny wirtualnej uruchomionej z kopii zapasowej w stałą maszynę wirtualną. Fizycznie oznacza to odzyskanie wszystkich dysków maszyny wirtualnej, a także zmian, które zaszły w czasie działania maszyny, do magazynu danych przechowującego te zmiany.

Format jednoplikowej kopii zapasowej

Format kopii zapasowych, w którym początkowa pełna kopia zapasowa i późniejsze przyrostowe kopie zapasowe są zapisywane w jednym pliku .tibx. W formacie tym wykorzystano szybkość metody tworzenia przyrostowych kopii zapasowych, unikając

© Acronis International GmbH, 2003-2024

najpoważniejszej wady tej metody — trudności związanych z usuwaniem przestarzałych kopii zapasowych. Oprogramowanie oznacza bloki zajmowane przez przestarzałe kopie zapasowe jako „wolne" i korzysta z nich podczas zapisywania nowych kopii zapasowych. Umożliwia to nadzwyczaj szybkie czyszczenie przy minimalnym obciążeniu zasobów. Ten format jednoplikowej kopii zapasowej nie jest dostępny w przypadku tworzenia kopii zapasowej w lokalizacji nieobsługujących odczytu i zapisu z dostępem losowym.

K

Komputer fizyczny

Komputer, którego kopie zapasowe są tworzone przez agenta zainstalowanego w systemie operacyjnym.

L

Lokalizacja lokalna

[Disaster Recovery] Lokalna infrastruktura zainstalowana w obiekcie danej firmy.

Lokalizacja w chmurze (lub lokalizacja odzyskiwania po awarii)

[Disaster Recovery] Lokalizacja zdalna w chmurze używana do obsługi infrastruktury odzyskiwania w razie wystąpienia awarii.

M

Maszyna wirtualna

Maszyna wirtualna, której kopie zapasowe są tworzone na poziomie hiperwizora przez agenta zewnętrznego, takiego jak agent dla VMware lub agent dla Hyper- V. Maszyna wirtualna zawierająca agenta jest z perspektywy tworzenia kopii zapasowych traktowana jak komputer fizyczny.

Moduł

Moduł jest elementem planu ochrony udostępniającym określoną funkcję ochrony danych, na przykład moduł Kopia zapasowa, moduł Ochrona przed wirusami i złośliwym oprogramowaniem itd.

Moduł kontroli urządzeń

Będąc elementem planu ochrony, moduł kontroli urządzeń na każdym komputerze korzysta z funkcji agenta ochrony przed utratą danych w celu wykrywania oraz blokowania nieuprawnionego dostępu do danych i ich przesyłania za pośrednictwem kanałów komputera lokalnego. Obejmują one dostęp użytkownika do urządzeń peryferyjnych i portów, drukowanie dokumentów, operacje kopiowania/wklejania przy użyciu schowka, operacje formatowania i wysuwania nośników, a także synchronizację z lokalnie podłączonymi urządzeniami mobilnymi. Moduł kontroli urządzeń zapewnia granularną, kontekstową kontrolę nad typami urządzeń i portami, do których użytkownicy mają dostęp na chronionym komputerze, oraz nad działaniami, które użytkownicy mogą podejmować na tych urządzeniach.

O

Ochrona przed utratą danych (wcześniej: ochrona przed wyciekiem danych)

System zintegrowanych technologii oraz środków organizacyjnych mających na celu wykrywanie i blokowanie przypadkowego bądź celowego ujawniania poufnych, chronionych lub wrażliwych danych albo uzyskiwania do nich dostępu przez nieuprawnione podmioty z

© Acronis International GmbH, 2003-2024

zewnątrz lub wewnątrz organizacji, a także przekazywania takich danych do niezaufanych środowisk.

Osierocona kopia zapasowa

Osierocona kopia zapasowa to kopia zapasowa, która nie jest już powiązana z żadnym planem ochrony.

P

Pełna kopia zapasowa

Samowystarczalna kopia zapasowa zawierająca wszystkie dane wybrane do uwzględnienia w niej. Aby odzyskać dane z pełnej kopii zapasowej, nie trzeba korzystać z żadnej innej kopii.

Plan ochrony

Plan ochrony to plan, który łączy w sobie moduły ochrony danych, takie jak: Kopia zapasowa, Ochrona przed wirusami i złośliwym oprogramowaniem, Filtrowanie adresów URL, Program antywirusowy Windows Defender, Microsoft Security Essentials, Ocena luk w zabezpieczeniach, Zarządzanie poprawkami, Mapa ochrony danych, Kontrola urządzeń.

Połączenie point-to-site (P2S)

[Disaster Recovery] Bezpieczne połączenie VPN z zewnątrz do lokalizacji w chmurze i lokalizacji lokalnej nawiązywane z urządzeń końcowych (np. komputera stacjonarnego lub laptopa).

Połączenie site-to-site (S2S)

[Disaster Recovery] Połączenie rozszerzające sieć lokalną o chmurę przy użyciu bezpiecznego tunelu VPN.

Powrót po awarii

Przełączenie obciążenia z zapasowego serwera (np. repliki maszyny wirtualnej lub serwera odzyskiwania w chmurze) z powrotem na serwer produkcyjny.

Przełączanie awaryjne

Przełączenie obciążenia z serwera produkcyjnego na zapasowy serwer (np. replikę maszyny wirtualnej lub serwer odzyskiwania w chmurze).

Przyrostowa kopia zapasowa

Kopia zapasowa, która zapisuje dane zmienione względem najnowszej kopii zapasowej. Aby odzyskać dane z przyrostowej kopii zapasowej, potrzebny jest dostęp do innych kopii zapasowych.

Publiczny adres IP

[Disaster Recovery] Adres IP przypisywany serwerowi chmurowemu, aby był on dostępny z Internetu.

R

Różnicowa kopia zapasowa

W różnicowej kopii zapasowej są przechowywane tylko dane zmienione względem ostatniej pełnej kopii zapasowej. Aby odzyskać dane z różnicowej kopii zapasowej, należy uzyskać dostęp do odpowiedniej pełnej kopii zapasowej.

Runbook

[Disaster Recovery] Planowany scenariusz obejmujący konfigurowalne czynności automatyzujące operacje związane z odzyskiwaniem po awarii.

© Acronis International GmbH, 2003-2024

S

Serwer chmurowy

[Disaster Recovery] Ogólne pojęcie oznaczające serwer odzyskiwania lub serwer podstawowy.

Serwer odzyskiwania

[Disaster Recovery] Replika oryginalnego komputera utworzona w formie maszyny wirtualnej na podstawie przechowywanych w chmurze kopii zapasowych chronionego serwera. Serwery odzyskiwania służą do przełączania obciążeń z oryginalnych serwerów w razie wystąpienia awarii.

Serwer podstawowy

[Disaster Recovery] Maszyna wirtualna, z którą nie jest powiązana żadna maszyna w lokalizacji lokalnej (np. serwer odzyskiwania). Serwery podstawowe służą do ochrony aplikacji lub obsługi różnych usług pomocniczych (np. serwera internetowego).

Sieć produkcyjna

[Disaster Recovery] Sieć wewnętrzna rozszerzona przy użyciu tunelowania VPN i obejmująca zarówno lokalizację lokalną, jak i lokalizację w chmurze. Serwery lokalne i chmurowe mogą komunikować się ze sobą w ramach sieci produkcyjnej.

Sieć testowa

[Disaster Recovery] Odizolowana sieć wirtualna służąca do testowania przełączania awaryjnego.

Sprawdzanie poprawności

Operacja sprawdzająca, czy można odzyskać dane z kopii zapasowej. Sprawdzanie poprawności kopii zapasowej plików jest operacją symulującą odzyskiwanie wszystkich plików z kopii zapasowej do tymczasowego miejsca docelowego. Sprawdzanie poprawności kopii zapasowej dysku polega na obliczeniu sumy kontrolnej każdego bloku danych zapisanego w kopii zapasowej. W obu procedurach są intensywnie wykorzystywane zasoby komputera. Pomyślny wynik sprawdzania poprawności oznacza wysokie prawdopodobieństwo poprawnego odzyskania danych, ale taka kontrola nie obejmuje weryfikacji wszystkich czynników wpływających na proces odzyskiwania.

T

Testowy adres IP

[Disaster Recovery] Adres IP potrzebny do testów przełączania awaryjnego, aby zapobiec zdublowaniu adresu IP ze środowiska produkcyjnego.

U

Urządzenie VPN

[Disaster Recovery] Specjalna maszyna wirtualna umożliwiająca połączenie między siecią lokalną a lokalizacją w chmurze przez bezpieczny tunel VPN. Urządzenie VPN jest wdrażane w lokalizacji lokalnej.

Z

Zestaw kopii zapasowych

Grupa kopii zapasowych, do których można zastosować odrębną regułę przechowywania. W przypadku schematu tworzenia kopii zapasowych Niestandardowy zestawy kopii zapasowych odpowiadają metodom tworzenia kopii zapasowych (Pełna, Różnicowa i Przyrostowa). W innych przypadkach

© Acronis International GmbH, 2003-2024

zestawami kopii zapasowych są grupy Co miesiąc, Codziennie, Co tydzień oraz Co godzinę. Miesięczną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu miesiąca. Tygodniową kopią zapasową jest pierwsza kopia zapasowa utworzona w dniu tygodnia wybranym w polu Tygodniowa kopia zapasowa (kliknij ikonę koła zębatego, a następnie Opcje tworzenia kopii zapasowych > Tygodniowa kopia zapasowa). Jeśli tygodniowa kopia zapasowa jest pierwszą kopią zapasową utworzoną po rozpoczęciu miesiąca, jest ona uznawana za miesięczną kopię zapasową. W takiej sytuacji tygodniowa kopia zapasowa zostanie utworzona w wybrany dzień następnego tygodnia. Dzienną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu dnia, chyba że spełnia warunki definicji miesięcznej lub tygodniowej kopii zapasowej. Godzinną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu godziny, chyba że spełnia warunki definicji miesięcznej, tygodniowej lub dziennej kopii zapasowej.

© Acronis International GmbH, 2003-2024

Indeks

3

32- czy 64-bitowy? 762

A

Active Protection 882

Active Protection w wersji Cyber Backup Standard 898

Administrowanie organizacjami Microsoft 365 dodanymi na różnych poziomach 652

Advanced Data Loss Prevention 928

Agent dla Hyper-V 29

Agent dla modułu Advanced Data Loss Prevention 26

Agent dla MySQL/MariaDB 27

Agent dla oVirt 30

Agent dla oVirt — wymagane role i porty 170

Agent dla programu Exchange (na potrzeby kopii zapasowych skrzynek pocztowych) 26

Agent dla programu Oracle 27

Agent dla rozwiązania Data Loss Prevention 25

Agent dla Scale Computing HC3 30

Agent dla Scale Computing HC3 (urządzenie wirtualne) — wymagane role 154

Agent dla SQL, agent dla usługi Active Directory, agent dla programu Exchange (na potrzeby kopii zapasowych baz danych oraz kopii zapasowych uwzględniających aplikacje) 25

Agent dla Synology 30

Agent dla systemu File Sync & Share 26

Agent dla systemu Linux 27

Agent dla systemu Mac 28

Agent dla systemu Windows 23

Agent dla usługi Microsoft 365 26

Agent dla Virtuozzo 30

Agent dla Virtuozzo Hybrid Infrastructure 30

Agent dla VMware — tworzenie kopii zapasowych bez obciążania sieci lokalnej 735

Agent dla VMware (urządzenie wirtualne) 29

Agent dla VMware (Windows) 29

Agent w chmurze i agent lokalny 641

Aktualizowanie agenta dla Synology 177

Aktualizowanie agentów ochrony 137

Aktualizowanie agentów ochrony na maszynach zaszyfrowanych przy użyciu funkcji BitLocker 142

Aktualizowanie definicji Cyber Protection na żądanie 196

Aktualizowanie definicji Cyber Protection według harmonogramu 196

Aktualizowanie, odbudowywanie lub usuwanie indeksów 710

Aktywacja konta 19

Aktywne połączenia point-to-site 829

Aktywowanie programu Startup Recovery Manager 783

Alerty 482

Alerty dotyczące kopii zapasowych 254

Alerty dotyczące licencjonowania 271

Alerty dotyczące modułu EDR 273

© Acronis International GmbH, 2003-2024

Alerty dotyczące modułu Filtrowanie adresów URL 272

Alerty dotyczące monitorowania 1168

Alerty dotyczące ochrony przed złośliwym oprogramowaniem 266

Alerty dotyczące odzyskiwania po awarii 259

Alerty dotyczące statusów kondycji dysków 288

Alerty dotyczące systemu 275

Alerty związane z kontrolą urządzeń 274, 383

Algorytm dystrybucji 739

Alokowanie dysków 733

Amazon 44

Analizowanie szczegółów incydentu 969

Aplikacje w chmurze 293

Atrybuty wyszukiwania obciążeń innych niż międzychmurowe 342

Atrybuty wyszukiwania obciążeń międzychmurowych 341

Automatyczne aktualizacje komponentów 195

Automatyczne aktualizowanie agentów ochrony 140

Automatyczne dodawanie pozycji do białej listy 922

Automatyczne testowe przełączanie awaryjne 839, 842

Automatyczne uruchamianie skryptów poprzedzających zablokowanie i następujących po odblokowaniu 742

Automatyczne usuwanie nieużywanych środowisk klientów w lokalizacji w chmurze 807

Automatyczne wykrywanie komputerów 181

Automatyczne wykrywanie miejsca docelowego 942

Automatyczne wyszukiwanie sterowników 547

Automatyczne zatwierdzanie poprawek 1053

B

Baza danych urządzeń USB 378

Bezpieczne odzyskiwanie 535

Blokada przechowywania 46

Brak pomyślnie utworzonych kopii zapasowych przez określoną liczbę kolejnych dni 482

Brakujące aktualizacje według kategorii 292

Brama VPN 801, 806

C

calculate hash 504

CBT (Changed Block Tracking) 490, 733

Chronienie danych usługi Hosted Exchange 637

Chronienie danych z baz MySQL i MariaDB 713

Chronienie kontrolera domeny 600

Chronienie programów Microsoft SQL Server i Microsoft Exchange Server 599

Chronione informacje dotyczące zdrowia (PHI) 943

Ciągła ochrona danych 437

Citrix 39

Co dalej 794

Co jest potrzebne do skorzystania z kopii zapasowej uwzględniającej aplikacje? 610

Co jest potrzebne do utworzenia kopii zapasowej witryny internetowej? 720

Co nowego w konsoli Cyber Protect 314

Co oznacza ochrona danych pakietu Google Workspace? 686

© Acronis International GmbH, 2003-2024

Co powoduje wyzwolenie reguły? 933

Co to jest plik kopii zapasowej? 483

Co to jest wąskie gardło? 575

Co trzeba wiedzieć 634

Co trzeba wiedzieć o finalizacji 728

Co trzeba wiedzieć o konwersji 245

Co zawiera kopia zapasowa dysku lub woluminu? 430

Cofanie przypisania poświadczeń z obciążenia 1099

Cyber Disaster Recovery Cloud — informacje 786

Cyber Protect Monitor 30, 305

Cyber Protection 277

Czy wymagane pakiety są już zainstalowane? 75

Czym dokładnie są incydenty? 965

Czynności 935

Czynności domyślne 916

Czynności dotyczące planów ochrony 224

Czynności w ramach reagowania dotyczące indywidualnych węzłów z cybernetycznego łańcucha zabijania 1007

Czyszczenie 242

D

Dane do analizy śledczej 496

Dane osobowe (PII) 944

Dane uznawane za chronione informacje dotyczące zdrowia 943

Dane uznawane za dane osobowe (PII) 945

Dane uznawane za PCI DSS 947

Data i godzina plików 561

Deduplikacja danych 60

Deduplikacja w archiwum 489

Definicje poufnych danych 943

Definiowanie czynności w ramach reagowania dotyczących obciążeń, które ucierpiały wskutek ataku 1009

Definiowanie czynności w ramach reagowania dotyczących podejrzanego pliku 1025

Definiowanie czynności w ramach reagowania dotyczących podejrzanego procesu 1021

Definiowanie czynności w ramach reagowania dotyczących podejrzanego wpisu rejestru 1026

Definiowanie lokalizacji kopii zapasowych na platformie Amazon S3 582

Definiowanie lokalizacji kopii zapasowych na platformie Microsoft Azure 579

Definiowanie lokalizacji kopii zapasowych na platformie Wasabi 584

Dezaktywowanie programu Startup Recovery Manager 784

Dlaczego istnieją miesięczne kopie zapasowe ze schematem godzinowym? 469

Dlaczego potrzebne jest rozwiązanie Endpoint Detection and Response (EDR) 958

Dlaczego warto korzystać z kopii zapasowej uwzględniającej aplikacje? 610

Dlaczego warto korzystać z narzędzia Bootable Media Builder? 762

Dlaczego warto korzystać z runbooków? 868

Dlaczego warto korzystać ze strefy Secure Zone? 443

Dlaczego warto tworzyć kopie zapasowe danych Microsoft 365? 641

© Acronis International GmbH, 2003-2024

Dodatkowe czynności dotyczące planów monitorowania 1162

Dodatkowe czynności w ramach istniejących już planów zarządzania zdalnego 1092

Dodatkowe narzędzia Cyber Protection 1180

Dodatkowe opcje planowania 464

Dodatkowe parametry 114

Dodatkowe wymagania dotyczące kopii zapasowych uwzględniających aplikacje 602

Dodatkowe wymagania w przypadku komputerów z systemami operacyjnymi Windows 612

Dodatkowe wymaganie dotyczące maszyn wirtualnych 611

Dodawanie dostępu do połączenia z chmurą publiczną 595

Dodawanie dostępu do subskrypcji platformy Microsoft Azure 592

Dodawanie lub usuwanie procesu, pliku bądź sieci na liście zablokowanych lub dozwolonych planu ochrony 1027

Dodawanie lub usuwanie urządzeń USB w ramach bazy danych 367

Dodawanie obciążenia do planu zarządzania zdalnego 1091

Dodawanie obciążeń do grupy statycznej 338

Dodawanie obciążeń do konsoli Cyber Protect 325

Dodawanie obciążeń do planów monitorowania 1159

Dodawanie organizacji Google Workspace 688

Dodawanie organizacji Microsoft 365 647, 651

Dodawanie plików poddanych kwarantannie do białej listy 922

Dodawanie poświadczeń 1098

Dodawanie sieci VLAN 777

Dodawanie zmiennej AR_RETENTION_LOCK_SUPPORT 46

Dołączanie baz danych programu SQL Server 622

Domyślna nazwa pliku kopii zapasowej 485

Domyślne opcje tworzenia kopii zapasowej 478

Dostęp do urządzenia wirtualnego za pomocą klienta SSH 180

Dostęp do złośliwych witryn internetowych 908

Dostęp VPN do lokalizacji lokalnej 828

Dostępne opcje odzyskiwania 558

Dostępne opcje tworzenia kopii zapasowych 479

Dostosowywanie uprawnień w regułach przepływów danych 933

Dynamiczna instalacja i dezinstalacja komponentów 82

Działania na serwerze podstawowym 862

Działanie narzędzia Universal Restore 548

Działanie po wykryciu 899

Dzielenie 525

Dziennik zdarzeń systemu Windows 531, 566

Dzierżawcy w trybie zgodności 555

E

Edytowanie domyślnych parametrów serwera odzyskiwania 795

Edytowanie grupy dynamicznej 357

Edytowanie lub usuwanie skryptu 409

Edytowanie planu ochrony 225

© Acronis International GmbH, 2003-2024

Eksportowanie kopii zapasowych 571

Elementy do skanowania 1037

Elementy do zreplikowania 232

Elementy, które można uwzględnić w kopii zapasowej 634

Endpoint Detection and Response (EDR) 957

F

Filtrowanie adresów URL 906

Filtry plików (uwzględniające/wykluczające) 494

Filtry uwzględniające i wykluczające 494

Finalizacja a zwykłe odzyskiwanie 728

Finalizacja maszyn uruchomionych z kopii zapasowych w chmurze 728

Finalizowanie maszyny 727

Firmowa biała lista 921

Fizyczne dostarczanie danych 517

Flashback 562

Format kopii zapasowej 488

Format kopii zapasowej i pliki kopii zapasowej 488

Funkcje 959

Funkcje antywirusowe 879

G

Gdzie mogę zobaczyć nazwy plików kopii zapasowej? 484

Generator nośnika startowego 762

Generowanie alertów, gdy dojdzie do złamania zabezpieczeń 959

Generowanie tokenu rejestracji 129

get content 503

Grupy dynamiczne 335

Grupy międzychmurowe i inne niż międzychmurowe 336

Grupy niestandardowe 335

Grupy słów kluczowych 949

Grupy statyczne 335

Grupy statyczne i grupy dynamiczne 335

Grupy urządzeń 334

Grupy wbudowane 334

Grupy wbudowane i grupy niestandardowe 334

H

H.264 1079

Harmonogram 301, 415, 1038, 1047

Harmonogram i warunki rozpoczęcia 415

Harmonogram jest oparty na zdarzeniach. 453

Harmonogram tworzenia kopii zapasowych 446

Historia instalacji poprawek 291

Historia ważności incydentów 280

Host lokalizacji kopii zapasowej jest dostępny 459

I

Ignoruj składniki zapisywania usługi VSS zakończone niepowodzeniem 528

Ignoruj uszkodzone sektory 493

Ile agentów jest wymaganych do tworzenia kopii zapasowej i odzyskiwania danych klastra? 606

Ile agentów potrzeba do utworzenia kopii zapasowej uwzględniającej klastry i odzyskania z niej danych? 609

© Acronis International GmbH, 2003-2024

Ile agentów potrzebuję? 146, 150, 156, 164

Indeksy wyszukiwania 710

Indywidualne plany ochrony do hostingu integracji panelu kontrolnego 229

Informacje dla administratorów partnerów 329

Informacje o harmonogramie tworzenia kopii zapasowych 687

Informacje o usłudze Fizyczne dostarczanie danych 517

Infrastruktura sieci w chmurze 796

Instalacja 88

Instalacja nienadzorowana i odinstalowywanie przy użyciu pliku EXE 92

Instalacja nienadzorowana i odinstalowywanie przy użyciu pliku MSI 100

Instalowanie agenta dla Synology 172

Instalowanie agentów i komponentów (połączenie MSI i MST) 101

Instalowanie agentów ochrony przy użyciu graficznego interfejsu użytkownika 84

Instalowanie agentów ochrony w systemie Linux 87

Instalowanie agentów ochrony w systemie macOS 89

Instalowanie agentów ochrony w systemie Windows 84

Instalowanie i odinstalowywanie agentów ochrony przy użyciu interfejsu wiersza polecenia 92

Instalowanie i odinstalowywanie agentów ochrony w systemie Linux 110

Instalowanie i odinstalowywanie agentów ochrony w systemie macOS 116

Instalowanie i odinstalowywanie agentów ochrony w systemie Windows 92

Instalowanie i wdrażanie agentów Cyber Protection 63

Instalowanie oraz odinstalowywanie agentów i komponentów (EXE) 92

Instalowanie oraz odinstalowywanie agentów i komponentów (MSI i wybór bezpośredni) 102

Instalowanie pakietów z repozytorium 76

Instalowanie poprawek na żądanie 1058

Integracje z rozwiązaniami DirectAdmin, cPanel i Plesk 724

Inteligentna ochrona 297

Interakcja z innymi opcjami tworzenia kopii zapasowych 521

Inwentaryzacja oprogramowania 1061

Inwentaryzacja sprzętu 1065

J

Jak działa routing 798, 801, 806

Jak działa wykrywanie automatyczne 181

Jak działa zdalna instalacja agentów 183

Jak korzystać z funkcji notaryzacji 477, 708

Jak odzyskać dane na urządzenie mobilne 635

Jak pliki trafiają do folderu kwarantanny? 920

Jak pobrać dane do analizy śledczej z kopii zapasowej? 498

Jak poddać incydenty dochodzeniu w cybernetycznym łańcuchu zabijania 986

Jak przeanalizować, które incydenty naruszenia bezpieczeństwa niezwłocznie wymagają uwagi 966

Jak przeglądać dane za pomocą konsoli Cyber Protect 636

Jak przypisać prawa użytkownika 87

© Acronis International GmbH, 2003-2024

Jak rozpocząć tworzenie kopii zapasowej danych 635

Jak się poruszać po etapach ataku 991

Jak to działa? 954

Jak usunąć strefę Secure Zone 446

Jak utworzenie strefy Secure Zone wpływa na dysk 444

Jak utworzyć strefę Secure Zone 445

Jak uzyskać aplikację Cyber Protect 635

Jak wykonać przełączenie awaryjne serwera DHCP 846

Jak wykonać przełączenie awaryjne serwerów korzystających z lokalnego serwera DNS 846

Jak zredukować wąskie gardła 576

Jakie elementy można odzyskać? 637, 649, 655, 666, 671, 675, 695, 700, 704

Jakie elementy można uwzględnić w kopii zapasowej? 637, 649, 655, 666, 670, 675, 695, 699, 703, 720

Jakie informacje są dostępne w ramach etapu ataku? 991

Jakiego typu kopii zapasowej potrzebuję? 66

Język zapytań Acronis XDR (XQL) 972

K

Kanał dotyczący zagrożeń 297

Karta Alerty 316

Karta Działania 304, 317

Karta Magazyn kopii zapasowych 566

Karta Urządzenia 317

Karta Zarządzanie oprogramowaniem 317

Kategorie do filtrowania 908

Klonowanie skryptu 408

Klucze dostępu 589, 591

Koder-dekoder adaptacyjny 1079

Kompatybilność formatów kopii zapasowych w różnych wersjach produktu 489

Kompatybilność modułu Odzyskiwanie po awarii z programami szyfrującymi 790

Kompatybilność z programami szyfrującymi 44

Kompatybilność z urządzeniami pamięci masowej Dell EMC Data Domain 45

Komponenty do instalacji nienadzorowanej (EXE) 99

Komponenty do instalacji nienadzorowanej (MSI) 108

Komputer fizyczny na maszynę wirtualną 538

Komputery z lukami w zabezpieczeniach 289

Konfiguracja sieci bramy VPN 801

Konfigurowalne monitory 1121

Konfigurowanie alertów dotyczących monitorowania 1168

Konfigurowanie automatycznego testowego przełączania awaryjnego 843

Konfigurowanie automatycznego zatwierdzania poprawek 1053

Konfigurowanie automatycznych czynności w ramach reagowania 1160

Konfigurowanie czasu występowania poprawki na liście 1052

Konfigurowanie funkcji odzyskiwania po awarii 792

Konfigurowanie kont użytkowników w środowisku Virtuozzo Hybrid Infrastructure 157

Konfigurowanie kopii zapasowej uwzględniającej aplikacje 714

© Acronis International GmbH, 2003-2024

Konfigurowanie liczby ponownych prób w przypadku wystąpienia błędu 241

Konfigurowanie łączności 797

Konfigurowanie niestandardowych serwerów DNS 826

Konfigurowanie obiektu zasad grupy 144

Konfigurowanie ochrony przed wirusami i złośliwym oprogramowaniem 875

Konfigurowanie operacji tworzenia kopii zapasowych CDP 440

Konfigurowanie planu ochrony Poprawki produkcyjne 1056

Konfigurowanie planu ochrony Poprawki testowe 1055

Konfigurowanie połączenia IPsec VPN multi-site 810

Konfigurowanie połączenia Open VPN site-to-site 808-809

Konfigurowanie reguł przechowywania 471

Konfigurowanie routingu lokalnego 827

Konfigurowanie serwerów odzyskiwania 835

Konfigurowanie serwerów podstawowych 859

Konfigurowanie sieci w środowisku Virtuozzo Hybrid Infrastructure 156

Konfigurowanie szyfrowania jako właściwości komputera 475

Konfigurowanie szyfrowania w planie ochrony 474

Konfigurowanie trybu Tylko chmura 808

Konfigurowanie trybu wyświetlania 778

Konfigurowanie urządzenia wirtualnego 147, 152, 160, 167

Konfigurowanie ustawień połączenia IPsec VPN multi-site 811

Konfigurowanie ustawień programu Klient rozwiązania Connect 1117

Konfigurowanie ustawień protokołu RDP 1100

Konfigurowanie ustawień serwera proxy 78

Konfigurowanie ustawień serwera proxy w narzędziu Cyber Protect Monitor 307

Konfigurowanie ustawień sieciowych 777

Konfigurowanie zasad powiadamiania pocztą e-mail 1176

Konfigurowanie zdalnego dostępu VPN point-to-site 817

Konflikt między nowym a wcześniejszym planem 228

Konflikt między planem indywidualnym a planem grupy 229

Konsola Cyber Protect 313

Konsolidacja kopii zapasowych 482

Kontroler domeny usługi Active Directory na potrzeby łączności L2 Open VPN 816

Kontroler domeny usługi Active Directory na potrzeby łączności L3 IPsec VPN 816

Konwersja na maszynę wirtualną 243

Konwersja regularna na maszynę wirtualną a uruchamianie maszyny wirtualnej z kopii zapasowej 246

Kopia zapasowa 61, 424

Kopia zapasowa bazy danych 603

Kopia zapasowa przed aktualizacją 1050

Kopia zapasowa sektor po sektorze 525

Kopia zapasowa skrzynki pocztowej 612

Kopia zapasowa uwzględniająca aplikacje 609

Kopia zapasowa uwzględniająca klastry 608

Kopiowanie bibliotek programu Microsoft Exchange Server 632

© Acronis International GmbH, 2003-2024

Korzystanie z funkcji ochrony zaawansowanej 926

Korzystanie z konsoli Cyber Protect w przypadku administratora partnera 315

Korzystanie z kontroli urządzeń 363

Korzystanie z modułu kontroli urządzeń 360

Korzystanie z modułu pakietu Endpoint Detection and Response (EDR) 963

Korzystanie z paska narzędzi w oknie podglądu 1113

Korzystanie z zainstalowanego lokalnie agenta dla Office 365 647

Krok 1 63

Krok 2 63

Krok 3 63

Krok 4 63

Krok 5 64

Krok 6 65

Krótki przegląd na pulpicie nawigacyjnym 960

Kryteria filtrów 495

Które elementy są nieodzyskiwalne? 672

Który agent jest potrzebny? 67

Kwarantanna 886, 919

L

Limity 723

Linux 431

list backups 502

list content 503

Lista dozwolonych typów urządzeń 375

Lista dozwolonych urządzeń USB 377

Lista urządzeń USB na komputerze 381

Lokalizacja kwarantanny na komputerach 921

Lokalne operacje wykonywane przy użyciu nośnika startowego 777

Ł

Łączenie reguł przepływów danych 934

M

Mac 431

Magazyn z geograficzną nadmiarowością 1185

Mapa ochrony danych 288, 300

Mapa organizacji 954

Maszyny wirtualne Microsoft Azure i Amazon EC2 759

McAfee Endpoint Encryption i PGP Whole Disk Encryption 45

Mechanizm obliczania wyniku #CyberFit 392

Mechanizm zachowań 887

Metody sprawdzania poprawności 238

Microsoft 36

Microsoft Azure 44

Microsoft BitLocker Drive Encryption 45

Microsoft Exchange Server 491

Microsoft Security Essentials 915

Microsoft SQL Server 490

Migawka kopii zapasowej na poziomie plików 496

Migawka wielowoluminowa 508

Migawki pośrednie 247

Migracja komputera 754

Migracja przy użyciu nośnika startowego 758

Moduł Microsoft Defender Antivirus 915

Monitorowanie 251

© Acronis International GmbH, 2003-2024

Monitorowanie kondycji dysków 284

Monitorowanie kondycji i wydajności obciążeń 1120

Monitorowanie obciążeń przy użyciu funkcji przesyłania zrzutów ekranu 1107

Monitorowanie typu Wykrywanie anomalii 1121

Montowanie baz danych programu Exchange Server 625

Montowanie woluminów z kopii zapasowej 568

Możliwe zadania związane z repliką 730

N

Nadawanie priorytetów incydentom wymagającym natychmiastowej uwagi 965

Nagrywanie i odtwarzanie sesji zdalnych 1116

Najważniejsze funkcje 786

Naprawianie całego incydentu 1002

Naprawianie incydentów 1002

Naprawianie incydentów z fałszywych zgłoszeń 1006

Narzędzie „tibxread" do pobierania danych z kopii zapasowej 501

Narzędzie Universal Restore w systemie Linux 548

Narzędzie Universal Restore w systemie Windows 546

Nawiązywanie połączenia z komputerem uruchomionym z nośnika startowego 777

Nawiązywanie połączenia z obciążeniem zarządzanym przy użyciu klienta internetowego 1104

Nawiązywanie połączeń z obciążeniami niezarządzanymi przy użyciu adresów IP 1111

Nawiązywanie połączeń z obciążeniami niezarządzanymi przy użyciu aplikacji Acronis Quick Assist 1110

Nawiązywanie połączeń z obciążeniami zarządzanymi na potrzeby pulpitu zdalnego lub pomocy zdalnej 1101

Nawiązywanie połączeń z zarządzanymi obciążeniami na potrzeby pulpitu zdalnego lub pomocy zdalnej 1072

Nazwa pliku kopii zapasowej 483

Nazwy bez zmiennych 486

NEAR 1078

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb cichy) 493, 561

Nie uruchamiaj przy połączeniu taryfowym 462

Nie uruchamiaj przy połączeniu z następującymi sieciami Wi-Fi 463

Nieobsługiwane funkcje 1180

Niestandardowe kategorie poufności 952

Niestandardowy czy gotowy nośnik startowy? 759

Niezmienny magazyn 1182

Norma bezpieczeństwa danych w branży kart płatniczych (PCI DSS) 947

Nośnik startowy oparty na systemie Linux 762

Nośnik startowy oparty na systemie Linux czy na środowisku WinPE/WinRE? 760

Nośnik startowy oparty na środowisku WinPE i WinRE 771

Notaryzacja 477, 708

Notaryzacje kopii zapasowych z danymi do analizy śledczej 499

© Acronis International GmbH, 2003-2024

Nutanix 42

O

Obciążenia 323

Obciążenia CyberApp 388

Obciążenia zagregowane 388

Obcinanie dziennika 506

Obiekt najwyższego poziomu 767

Obiekt zmiennej 768

Obrazy WinPE 772

Obrazy WinRE 771

Obserwacja wyniku redystrybucji 740

Obserwowanie wielu obciążeń zarządzanych naraz 1108

Obsługa błędów 492, 561, 734

Obsługa funkcji ochrony w poszczególnych systemach operacyjnych 47

Obsługa migracji maszyn wirtualnych 743

Obsługa niepowodzenia zadania 526

Obsługa wielu dzierżawców 322

Obsługiwane funkcje na platformach 876

Obsługiwane funkcje pulpitu zdalnego i pomocy zdalnej 1074

Obsługiwane języki 943-944, 947-948

Obsługiwane klasy magazynów 588

Obsługiwane konfiguracje klastrów 606, 608

Obsługiwane lokalizacje 233-234, 242, 473

Obsługiwane lokalizacje docelowe 440

Obsługiwane operacje na woluminach logicznych 61

Obsługiwane platformy 399, 875, 1077

Obsługiwane platformy wirtualizacji 32, 787

Obsługiwane produkty dla systemu Linux 1037

Obsługiwane produkty firmy Apple 1036

Obsługiwane produkty firmy Apple i innych firm 1036

Obsługiwane produkty firmy Microsoft 1035

Obsługiwane produkty firmy Microsoft i innych firm 1035

Obsługiwane produkty innych firm dla systemu macOS 1037

Obsługiwane produkty innych firm przeznaczone do systemu operacyjnego Windows 1036

Obsługiwane przeglądarki internetowe 23

Obsługiwane systemy operacyjne 787

Obsługiwane systemy operacyjne i środowiska 23

Obsługiwane systemy operacyjne i wersje 47

Obsługiwane systemy operacyjne Windows 919

Obsługiwane systemy plików 57

Obsługiwane typy maszyn wirtualnych 245

Obsługiwane urządzenia mobilne 633

Obsługiwane wersje 685

Obsługiwane wersje platformy SAP HANA 32

Obsługiwane wersje programu Microsoft Exchange Server 31

Obsługiwane wersje programu Microsoft SharePoint 31

Obsługiwane wersje programu Microsoft SQL Server 30

Obsługiwane wersje programu MySQL 32

Obsługiwane wersje systemu MariaDB 32

Obsługiwane wersje systemu Oracle Database 31

© Acronis International GmbH, 2003-2024

Obsługiwane źródła danych 439

Ocena luk w zabezpieczeniach 1034

Ocena luk w zabezpieczeniach i zarządzanie poprawkami 1034

Ocena luk w zabezpieczeniach komputerów z systemem Windows 1040

Ocena luk w zabezpieczeniach urządzeń z systemem macOS 1041

Ocena luk w zabezpieczeniach w przypadku komputerów z systemem Linux 1041

Ochrona aplikacji do współpracy i komunikacji 249

Ochrona aplikacji firmy Microsoft 599

Ochrona danych Microsoft 365 641

Ochrona danych pakietu Google Workspace 686

Ochrona danych programu Exchange Online 655

Ochrona danych rozwiązania Gmail 695

Ochrona folderów sieciowych 883

Ochrona grup dostępności bazy danych (DAG) 607

Ochrona instancji Microsoft 365 Teams 675

Ochrona notesów aplikacji OneNote 684

Ochrona platformy SAP HANA 712

Ochrona plików z Dysku Google 699

Ochrona plików z Dysku udostępnionego 703

Ochrona plików z magazynu OneDrive 666

Ochrona po stronie serwera 884

Ochrona programu Microsoft SharePoint 599

Ochrona przed exploitami 887

Ochrona przed wirusami i złośliwym oprogramowaniem 879

Ochrona serwerów hostingu witryn internetowych 723

Ochrona skrzynek pocztowych programu Exchange Online 649

Ochrona stanowisk aplikacji do współpracy Microsoft 365 685

Ochrona systemu Oracle Database 712

Ochrona środowisk wirtualizacji 743

Ochrona urządzeń mobilnych 633

Ochrona w czasie rzeczywistym 880, 889, 917

Ochrona witryn internetowych 720

Ochrona witryn internetowych i serwerów hostingu 720

Ochrona witryn programu SharePoint Online 670

Ochrona własna 885

Ochrona zawsze włączonych grup dostępności (AAG) 606

Odinstalowywanie agentów 90

Odnawianie dostępu do połączenia z chmurą publiczną 597

Odnawianie dostępu do subskrypcji platformy Microsoft Azure 593

Odnawianie zasad dla firmy lub jednostki 936

Odnawianie zasad dla wybranych użytkowników z firmy lub jednostki 937

Odnawianie zasad przepływów danych 936

Odnawianie zasad użytkownika przy użyciu trybu Egzekwowanie adaptacyjne 937

Odnawianie zasad użytkownika przy użyciu trybu obserwacji 937

Odwoływanie planów monitorowania 1160

Odwoływanie planu ochrony 226

Odwoływanie planu z grupy 359

© Acronis International GmbH, 2003-2024

Odzyskiwanie 62, 532

Odzyskiwanie — ściągawka 532

Odzyskiwanie aplikacji 600

Odzyskiwanie baz danych 717

Odzyskiwanie baz danych programu Exchange 623

Odzyskiwanie baz danych SQL 614

Odzyskiwanie baz danych SQL jako plików 619

Odzyskiwanie baz danych SQL na komputer inny niż pierwotny 617

Odzyskiwanie baz danych SQL na pierwotny komputer 615

Odzyskiwanie baz danych uwzględnionych w grupie AAG 607

Odzyskiwanie bazy danych master 622

Odzyskiwanie całego Dysku Google 701

Odzyskiwanie całego dysku OneDrive 668

Odzyskiwanie całego Dysku udostępnionego 705

Odzyskiwanie całego serwera 716

Odzyskiwanie całego zespołu 677

Odzyskiwanie całych skrzynek pocztowych do plików danych PST 661

Odzyskiwanie danych klastra programu Exchange 609

Odzyskiwanie danych z kopii zapasowej uwzględniającej aplikacje 715

Odzyskiwanie danych z programu SharePoint Online 673

Odzyskiwanie do kontenerów Virtuozzo lub maszyn wirtualnych Virtuozzo 556

Odzyskiwanie dysków przy użyciu nośnika startowego 544

Odzyskiwanie Dysku Google i plików z Dysku Google 701

Odzyskiwanie Dysku udostępnionego i plików z Dysku udostępnionego 705

Odzyskiwanie elementów skrzynki pocztowej 629, 640, 650, 659, 697

Odzyskiwanie elementów skrzynki pocztowej do plików PST 662

Odzyskiwanie elementów skrzynki pocztowej zespołu do plików PST 681

Odzyskiwanie folderów publicznych i elementów folderów 664

Odzyskiwanie instancji 716

Odzyskiwanie jednym kliknięciem 508

Odzyskiwanie kanałów zespołu lub dostępnych w nich plików 678

Odzyskiwanie komputera 536

Odzyskiwanie komputera przy użyciu funkcji Odzyskiwanie jednym kliknięciem 512

Odzyskiwanie komputerów fizycznych 536

Odzyskiwanie konfiguracji ESXi 557

Odzyskiwanie kopii zapasowych dla dzierżawców w trybie zgodności 1182

Odzyskiwanie lokalne przy użyciu nośnika startowego 778

Odzyskiwanie magazynu OneDrive i plików z magazynu OneDrive 668

Odzyskiwanie maszyny wirtualnej 540

Odzyskiwanie na inną platformę 533

Odzyskiwanie notesów aplikacji OneNote uwzględnionych w kopii zapasowej 684

Odzyskiwanie pełnej ścieżki 562

Odzyskiwanie plików 549

Odzyskiwanie plików przy użyciu nośnika startowego 554

© Acronis International GmbH, 2003-2024

Odzyskiwanie plików w konsoli Cyber Protect 549

Odzyskiwanie plików z Dysku Google 702

Odzyskiwanie plików z Dysku udostępnionego 706

Odzyskiwanie plików z magazynu OneDrive 669

Odzyskiwanie procedur składowanych 719

Odzyskiwanie skrzynek pocztowych 627, 639, 650, 658, 696

Odzyskiwanie skrzynek pocztowych i elementów skrzynek pocztowych 639, 650, 658, 696

Odzyskiwanie skrzynek pocztowych programu Exchange i ich elementów 626

Odzyskiwanie skrzynki pocztowej zespołu 680

Odzyskiwanie stanu systemu 556

Odzyskiwanie systemowych baz danych 621

Odzyskiwanie tabel 718

Odzyskiwanie wiadomości e-mail i spotkań 682

Odzyskiwanie witryny internetowej 722

Odzyskiwanie witryny zespołu lub poszczególnych elementów witryny 683

Odzyskiwanie z kopii zapasowej 1019

Odzyskiwanie z magazynu w chmurze 766

Odzyskiwanie z ponownym uruchomieniem 543

Odzyskiwanie z udziału sieciowego 766

Ogólne zalecenia dotyczące lokalizacji lokalnych 813

Ograniczanie łącznej liczby maszyn wirtualnych, których kopie zapasowe mogą być tworzone w tym samym czasie 753

Ograniczenia 34, 37, 39-40, 42-43, 156, 165, 172, 246, 284, 399, 429-430, 434, 437, 444, 535, 544, 551, 560, 645, 666, 671, 675, 688, 696, 699-700, 704, 713, 720, 730, 736, 783, 788, 924, 1180

Ograniczenia dotyczące odzyskiwania plików w konsoli Cyber Protect 555

Ograniczenia i znane problemy 685

Ograniczenia nazw plików kopii zapasowej 484

Ograniczenia w przypadku korzystania z magazynu Geo-redundant Cloud Storage 790

Okno na utworzenie kopii zapasowej 514

Określanie ustawień kanałów dotyczących zagrożeń 999

Omówienie procesu fizycznego dostarczania danych 518

Oparty na środowisku WinPE/WinRE 760

opartym na systemie Linux 760

Opcje dodatkowe 452

Opcje odzyskiwania 558

Opcje powrotu po awarii 734

Opcje replikacji 733

Opcje tworzenia kopii zapasowych 479

Operacje dotyczące kopii zapasowych 566

Operacje dotyczące maszyn wirtualnych Microsoft Azure 859

Operacje przy użyciu runbooków 872

Operacje zdalne dotyczące nośnika startowego 779

Operatory wyszukiwania 355

Opis 915

Opis opcji 504

Opis planów 207

Opis wykrywania wąskich gardeł 574

© Acronis International GmbH, 2003-2024

Oprogramowanie Microsoft Defender Antivirus i Microsoft Security Essentials 915

Oracle 41

Orkiestracja (runbooki) 868

Ostatnio dotknięte problemem 293

Oszczędzaj baterię 461

oVirt / Red Hat Virtualization 4.2 i 4.3 / Oracle Virtualization Manager 4.3 170

oVirt / Red Hat Virtualization 4.4, 4.5 170

Oznaczono jako poufne 948

P

Pakiety systemu Linux 74

Pamięć podręczna 197

Parallels 41

Parametry 763

Parametry dezinstalacji 115

Parametry dotyczące instalacji nienadzorowanej (EXE) 94

Parametry dotyczące instalacji nienadzorowanej (MSI) 104

Parametry dotyczące starszych funkcji 115

Parametry informacyjne 115

Parametry instalacji 112

Parametry instalacji nienadzorowanej lub dezinstalacji 112

Parametry jądra 763

Parametry rejestracji 113

Parametry runbooka 871

Parametry zdarzenia 456

Plan ochrony — ściągawka 426

Plany domyślne 217

Plany monitorowania 1120, 1156

Plany na różnych poziomach administracji 419

Plany obsługiwane w przypadku grup urządzeń 336

Plany ochrony danych poza hostem 230

Plany ochrony i moduły 221

Plany skanowania kopii zapasowych 247

Plany skryptów 412

Plany tworzenia kopii zapasowych aplikacji w chmurze 248

Plany wbudowane 208

Plany zarządzania zdalnego 1082

Platformy obsługiwane w ramach monitorowania 1121

Pliki dziennika IPsec VPN multi-site 834

Pliki skryptu 767

Po wybraniu opcji tworzenia maszyny wirtualnej na serwerze wirtualizacji 247

Po wybraniu opcji zapisu maszyny wirtualnej w postaci zestawu plików 247

Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows 456

Pobieranie agentów ochrony 74

Pobieranie danych dotyczących ostatnio dotkniętych problemem obciążeń 293

Pobieranie danych wyjściowych operacji wykonanej przy użyciu skryptu 411

Pobieranie dzienników bramy VPN 830

Pobieranie dzienników urządzenia VPN 830

Pobieranie plików dziennika IPsec VPN 834

Pobieranie plików z chmury 551

Pobieranie programu instalacyjnego 172

Pobierz konfigurację dla pakietu OpenVPN 828

© Acronis International GmbH, 2003-2024

Początkowa konfiguracja łączności 808

Poczekaj na spełnienie warunków z harmonogramu 527

Poddawanie dochodzeniu pojedynczych węzłów z cybernetycznego łańcucha zabijania 993

Poddawanie incydentów dochodzeniu 985

Podpisywanie pliku w usłudze ASign 552

Podstawowe parametry 112

Podsumowanie instalacji poprawek 291

Podział najliczniejszych incydentów według obciążeń 279

Pojęcia dotyczące sieci 797

Pola zdarzeń 977

Polecenia poprzedzające rejestrowanie danych/następujące po nim 521

Polecenia poprzedzające/następujące 519, 563, 734

Polecenie następujące po utworzeniu kopii zapasowej 520

Polecenie następujące po zarejestrowaniu danych 523

Polecenie po zakończeniu odzyskiwania 564

Polecenie poprzedzające odzyskiwanie 563

Polecenie poprzedzające rejestrowanie danych 522

Polecenie poprzedzające utworzenie kopii zapasowej 519

Połączenia SSH z urządzeniem wirtualnym 179

Połączenia z obciążeniami zdalnymi na potrzeby pulpitu zdalnego lub pomocy zdalnej 1081

Połączenie IPsec VPN multi-site 805

Połączenie lokalne 777

Połączenie Open VPN site-to-site 799, 818

Połączenie Open VPN site-to-site — dodatkowe informacje 198

Połączenie zdalne z obciążeniem 1018

Pomiń wykonywanie zadania 527

Ponowne generowanie konfiguracji 828

Ponowne instalowanie bramy VPN 822

Ponowne uruchamianie obciążenia 1016

Porównywanie wersji skryptu 411

Porty 809

Porty TCP wymagane do operacji tworzenia kopii zapasowych i replikacji maszyn wirtualnych VMware 64

Porty wymagane przez komponent Menedżer pobierania 65

Poświadczenia dostępu do obciążenia 1097

Powiadomienia dotyczące pulpitu zdalnego 1118

Powiadomienia systemu operacyjnego i alerty usługi 374

Powiązanie ręczne 740

Powrót po awarii na docelową maszynę wirtualną 847

Powrót po awarii na docelowy komputer fizyczny 852

Powszechna reguła dotycząca instalacji 45

Powszechna reguła dotycząca tworzenia kopii zapasowych 45

Poziom dzierżawcy-klienta 315

Poziom dzierżawcy-partnera (Wszyscy klienci) 315

Poziom dzierżawcy-partnera w konsoli Cyber Protect 316

Poznanie bieżącego poziomu ochrony 251

© Acronis International GmbH, 2003-2024

Poznawanie czynności podjętych w celu zniwelowania skutków incydentu 995

Praca w środowisku VMware vSphere 729

Praca z dziennikami 829

Praca z obciążeniami CyberApp 388

Praca z obciążeniami niezarządzanymi 1110

Praca z obciążeniami zagregowanymi 389

Praca z obciążeniami zarządzanymi 1100

Praca z planami 207

Praca z zaszyfrowanymi kopiami zapasowymi 858

Priorytet procesora 515

Problem z licencją 229

Problemy z kompatybilnością dotyczące planów monitorowania 1166

Problemy z kompatybilnością dotyczące planów skryptów 420

Problemy z kompatybilnością z planami zarządzania zdalnego 1095

Procedury odzyskiwania dotyczące konkretnych programów 45

Proces konfiguracji modułu Filtrowanie adresów URL 908

Proces tworzenia kopii zapasowej na potrzeby analizy śledczej 497

Produkcyjne przełączanie awaryjne 838

Produkty firmy Microsoft 1045

Produkty innych firm przeznaczone do systemu Windows 1046

Protokoły połączeń zdalnych 1078

Przebieg powrotu po awarii 847

Przebieg przełączania awaryjnego 838

Przechowywanie zdarzeń związanych z bezpieczeństwem przez 180 dni 961

Przechwytywanie pakietów sieciowych 831

Przed uruchomieniem odzyskiwania wyłącz docelowe maszyny wirtualne 565

Przegląd klastrów programu Exchange Server 607

Przegląd rozwiązań dla SQL Server o wysokiej dostępności 606

Przegląd zasad i zarządzanie nimi 935

Przeglądanie i analizowanie wykrytych wskaźników naruszenia zabezpieczeń 1001

Przeglądanie incydentów 964

Przeglądanie wskaźników naruszenia zabezpieczeń i niwelowanie skutków na obciążeniach, których dotyczy problem 1000

Przeglądanie wyników inwentaryzacji oprogramowania 1062

Przeglądanie wyników inwentaryzacji sprzętu 1067

Przekierowanie dźwięku w ramach połączenia zdalnego 1080

Przekierowywanie dźwięku z obciążenia zdalnego z systemem Linux 1081

Przekierowywanie dźwięku z obciążenia zdalnego z systemem macOS 1080

Przekierowywanie dźwięku z obciążenia zdalnego z systemem Windows 1080

Przełączanie awaryjne na replikę 732

Przełączanie awaryjne w ramach odzyskiwania po awarii 1020

Przenoszenie maszyn do innego dzierżawcy 137

Przepływ pracy zarządzania poprawkami 1044

Przeprowadzanie dochodzenia dotyczącego etapów ataku w ramach incydentu 990

© Acronis International GmbH, 2003-2024

Przesyłanie dźwięku 1079

Przesyłanie plików 1105

Przesyłanie plików za pośrednictwem aplikacji Acronis Quick Assist 1112

Przy użyciu chmurowego agenta dla usługi Microsoft 365 651

Przydatne porady 652, 689

Przygotowanie 63, 87, 546

Środowisko WinPE 2.x lub 3.x 774

środowisko WinPE 4.0 lub nowsze 774

Przygotowywanie komputera do instalacji zdalnej 187

Przygotuj sterowniki 546

Przykład 94, 104, 117, 158-159, 459-464, 470

Awaryjna kopia zapasowa po wykryciu uszkodzonych sektorów na dysku twardym 457

ręczne instalowanie pakietów w systemie Fedora 14 77

Przykładowe typy danych 976

Przykładowe zapytania 974

Przykłady 93-94, 102, 104, 116

Przykłady użycia 472, 725, 729, 741

Przypadek użycia automatycznego zatwierdzania poprawek bez testów 1057

Przypadek użycia automatycznego zatwierdzania poprawek i testów 1054

Przypisywanie poświadczeń do obciążenia 1099

Przystępne wizualizacje przebiegu ataku 960

Przywrócenie oryginalnego początkowego dysku RAM 549

Przyznawanie uprawnień dostępu do konta użytkownika 750

Przyznawanie wymaganych uprawnień systemowych modułowi Agent rozwiązania Connect 83

Publiczny i testowy adres IP 802

Pulpit nawigacyjny Alerty 253

Pulpit nawigacyjny Działania 252

Pulpit nawigacyjny Przegląd 251

Puls maszyny wirtualnej 239

Punkty obliczeniowe 791

Punkty zamontowania 507, 562

R

Raport o licencjonowaniu stanowisk Microsoft 365 646

Raportowane dane zależnie od typu widżetu 310

Raporty 307

RDP 1080

Red Hat i Linux 40

Redystrybucja 740

Reguły dotyczące dysków i woluminów 432

Reguły dotyczące plików i folderów 434

Reguły dotyczące rozszerzeń i wyjątków 303

Reguły przechowywania 467

Reguły przechowywania zgodnie ze schematem tworzenia kopii zapasowych 468

Reguły zapory dotyczące serwerów chmurowych 863

Rejestracja maszyn 127

Rejestrowanie i wyrejestrowywanie maszyn przy użyciu interfejsu wiersza polecenia 132

© Acronis International GmbH, 2003-2024

Rejestrowanie maszyn przy użyciu graficznego interfejsu użytkownika 127

Rejestrowanie maszyn przy użyciu konsoli Cyber Protect 127

Rejestrowanie maszyn przy użyciu poświadczeń użytkownika 128, 132

Rejestrowanie maszyn przy użyciu tokenu rejestracji 129, 134

Rejestrowanie nośnika startowego 775

Replikacja 472

Replikacja a tworzenie kopii zapasowej 729

Replikacja kopii zapasowej 230

Replikacja maszyn wirtualnych 729

Repozytorium skryptów 411

Resetowanie modeli uczenia maszynowego 1167

Ręczne aktualizowanie agentów ochrony 138

Ręczne czynności w ramach reagowania 1172

Ręczne dodawanie pozycji do białej listy 922

Ręczne instalowanie pakietów 77

Ręczne uruchamianie operacji tworzenia kopii zapasowej 466

Ręczne uruchamianie operacji tworzenia kopii zapasowej z chmury do chmury 249

Ręczne uruchamianie skanowania w celu inwentaryzacji oprogramowania 1062

Ręczne uruchamianie skanowania w celu inwentaryzacji sprzętu 1067

Ręczne zatwierdzanie poprawek 1058

Ręczny powrót po awarii 856

Role użytkowników a prawa do funkcji Skrypty cybernetyczne 400

Rozpoczęcie pracy z produktem Cyber Protection 19

Rozwiązywanie napotkanych problemów z konfiguracją IPsec VPN 832

Rozwiązywanie problemów 191, 544

Rozwiązywanie problemów z kompatybilnością dotyczących planów monitorowania 1166

Rozwiązywanie problemów z kompatybilnością dotyczących planów skryptów 420

Rozwiązywanie problemów z kompatybilnością z planami zarządzania zdalnego 1096

Rozwiązywanie problemów z konfiguracją IPsec VPN 831

Różne opcje logowania 1079

S

Samoobsługowy niestandardowy folder na żądanie 921

Scale Computing 39

Scenariusze użycia 569

Schematy tworzenia kopii zapasowych 447

Secure Zone — informacje 443

Seeding repliki początkowej 734

Serwery odzyskiwania 802

Serwery podstawowe 804

Sieciowe wymagania agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne) 156

Skanowanie antywirusowe kopii zapasowych 923

Skanowanie planowane 881

Składnia 972

Skrypty 402

Skrypty cybernetyczne 398

Skrypty na nośniku startowym 765

© Acronis International GmbH, 2003-2024

Skrypty niestandardowe 766

Specjalne operacje dotyczące maszyn wirtualnych 724

Sposób działania 284, 297, 300, 392, 437, 478, 500, 708, 898, 906

Sposób korzystania ze strefy Secure Zone 45

Sprawdzanie działań dotyczących zapory chmury 867

Sprawdzanie obciążeń pod kątem wystąpienia ujawnionych publicznie ataków za pomocą kanałów dotyczących zagrożeń 960

Sprawdzanie obciążeń pod kątem występowania wskaźników naruszenia zabezpieczeń (IOC) z publicznie znanych ataków 998

Sprawdzanie poprawności 234

Sprawdzanie poprawności kopii zapasowej 489, 559

Sprawdzanie poprawności kopii zapasowych 570

Sprawdzanie poprawności zrzutu ekranu 239

Sprawdzanie rozmiaru indeksu wyszukiwania 710

Sprawdzanie, czy pakiet Endpoint Detection and Response (EDR) poprawnie działa 1031

Sprawdź adres IP urządzenia 464

Sprawdź dostęp do sterowników w środowisku startowym 547

Startup Recovery Manager 782

Status georeplikacji 1186

Status instalacji poprawek 291

Status ochrony 277

Status sieciowy obciążeń 282

Status sprawdzanie poprawności 235

Status zagrożeń 279

Sterowniki pamięci masowej do zainstalowania mimo to 547

Stopień kompresji 492

Stosowanie planu do grupy 358

Stosowanie planu ochrony do obciążenia 225

Stosowanie poprawki do obciążenia 1014

Strona zarządzania bazą danych urządzeń USB 379

Struktura pliku autostart.json 767

Struktura reguł 931

Struktura zasad przepływów danych 931

Szczegóły skanowania kopii zapasowej 292

Szukaj wskaźników naruszenia zabezpieczeń (IoC) i podejrzanych działań 971

Szybka przyrostowa/różnicowa kopia zapasowa 494

Szybkie uruchomienie skryptu 421

Szybkość danych wyjściowych podczas tworzenia kopii zapasowej 517

Szyfrowanie 474

Ś

Średni czas rozwiązywania problemu incydentu bezpieczeństwa 281

Środowisko odzyskiwania 543

T

Testowanie repliki 731

Testuj przełączenie awaryjne 839

Tryb startowy 559

Tryb tworzenia kopii zapasowych klastra 490

© Acronis International GmbH, 2003-2024

Tryb Tylko chmura 798, 820

Tryb zgodności 1180

Tryby niezmiennego magazynu 1182

Tworzenie dynamicznej grupy urządzeń na poziomie partnera 318

Tworzenie fizycznego nośnika startowego 761

Tworzenie grupy dynamicznej 339

Tworzenie grupy statycznej 336

Tworzenie harmonogramu 524

Tworzenie kopii zapasowej danych klastra programu Exchange 609

Tworzenie kopii zapasowej witryny internetowej 720

Tworzenie kopii zapasowych baz danych uwzględnionych w grupie AAG 606

Tworzenie kopii zapasowych maszyn Hyper-V w klastrach 752

Tworzenie kopii zapasowych na platformie Amazon S3 588

Tworzenie kopii zapasowych na platformie Microsoft Azure 588

Tworzenie kopii zapasowych na platformie Wasabi 590

Tworzenie kopii zapasowych obciążeń w chmurach publicznych 579

Tworzenie kopii zapasowych przy użyciu agenta i bezagentowe 66

Tworzenie kopii zapasowych serwerów chmurowych 867

Tworzenie kopii zapasowych w już istniejącym archiwum kopii zapasowych 486

Tworzenie na żądanie kopii zapasowej na potrzeby analizy śledczej dla obciążenia 1017

Tworzenie nośnika startowego WinPE lub WinRE 772

Tworzenie nośników startowych do odzyskiwania systemów operacyjnych 759

Tworzenie osobistego projektu Google Cloud 689

Tworzenie planu monitorowania 1157

Tworzenie planu ochrony 222

Tworzenie planu ochrony na potrzeby odzyskiwania po awarii 793

Tworzenie planu replikacji 730

Tworzenie planu replikacji kopii zapasowej 231

Tworzenie planu skryptów 413

Tworzenie planu sprawdzania poprawności 235

Tworzenie planu zarządzania zdalnego 1083

Tworzenie pliku transformacji i wyodrębnianie pakietów instalacyjnych 144

Tworzenie runbooka 868

Tworzenie serwera odzyskiwania 835

Tworzenie serwera podstawowego 859

Tworzenie skryptu 403

Tworzenie skryptu przy użyciu AI 405

Tworzenie statycznej grupy urządzeń na poziomie partnera 318

Tworzenie zasad i reguł przepływów danych 928

Tygodniowa kopia zapasowa 531

Typ elementu sterującego 769

Typowe wymagania 601

Typy alertów 254

Typy i pola zdarzeń 975

© Acronis International GmbH, 2003-2024

Typy kopii zapasowych 449

Typy monitorowania 1120

Typy skanowania 880

Typy zdarzeń 975

U

Udostępnianie ekranu firmy Apple 1080

Ulubione plany 219

Umożliwianie korzystania z modułu kontroli urządzeń w systemie macOS 363

Uprawnienia 934

Uprawnienia wymagane do instalacji nienadzorowanej w systemie macOS 118

Uprawnienia wymagane w przypadku konta logowania 86

Uprawnienia związane z zasadami 589-590

Uruchamianie demona Secure Shell 179

Uruchamianie maszyny 725

Uruchamianie maszyny wirtualnej z kopii zapasowej (Instant Restore) 724

Uruchamianie operacji tworzenia kopii zapasowej zgodnie z harmonogramem 450

Uruchamianie planu ochrony Poprawki testowe i odrzucanie niebezpiecznych poprawek 1057

Uruchamianie skanowania w celu ustalenia wyniku #CyberFit 397

Uruchom jako maszynę wirtualną 238

Urządzenie VPN 802

Usługa kopiowania woluminów w tle (VSS) 527

Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych 529, 734

Usługi Cyber Protection instalowane w danym środowisku 197

Usługi instalowane w systemie macOS 198

Usługi instalowane w systemie Windows 197

Ustalanie zakresu i skutków incydentów 968

Ustawianie częstotliwości tworzenia kopii zapasowych danych Google Workspace 694

Ustawianie częstotliwości tworzenia kopii zapasowych danych pakietu Microsoft 365 654

Ustawianie hasła szyfrowania 1181

Ustawianie hasła użytkownika root na urządzeniu wirtualnym 180

Ustawianie planów jako domyślnych 218

Ustawianie planów jako ulubionych 219

Ustawianie reguł zapory dla serwerów chmurowych 864

Ustawienia białej listy 922

Ustawienia dostępu 369

Ustawienia dotyczące zasobników 590-591

Ustawienia modułu Filtrowanie adresów URL 908

Ustawienia modułu Mapa ochrony danych 301

Ustawienia modułu Ocena luk w zabezpieczeniach 1037

Ustawienia modułu Ochrona przed wirusami i złośliwym oprogramowaniem 881

Ustawienia monitora Dziennik zdarzeń systemu Windows 1150

Ustawienia monitora Miejsce na dysku 1127

Ustawienia monitora Niepowodzenia logowania 1152

Ustawienia monitora Niestandardowe 1155

© Acronis International GmbH, 2003-2024

Ustawienia monitora Ostatnie ponowne uruchomienie systemu 1149

Ustawienia monitora Poziom użycia pamięci 1135

Ustawienia monitora Poziom użycia pamięci przez proces 1144

Ustawienia monitora Poziom użycia procesora 1133

Ustawienia monitora Poziom użycia procesora przez proces 1143

Ustawienia monitora Poziom użycia sieci przez proces 1146

Ustawienia monitora Rozmiar plików i folderów 1151

Ustawienia monitora Status funkcji uruchamiania automatycznego 1155

Ustawienia monitora Status oprogramowania antywirusowego 1153

Ustawienia monitora Status procesu 1148

Ustawienia monitora Status usług systemu Windows 1147

Ustawienia monitora Status usługi Windows Update 1152

Ustawienia monitora Status zapory 1152

Ustawienia monitora Szybkość transferu dysku 1137

Ustawienia monitora Szybkość transferu dysku generowanego przez proces 1145

Ustawienia monitora Temperatura procesora 1130

Ustawienia monitora Temperatura procesora graficznego 1131

Ustawienia monitora Wykorzystanie sieci 1140

Ustawienia monitora Zainstalowane oprogramowanie 1148

Ustawienia monitora Zmiany sprzętowe 1133

Ustawienia narzędzia Universal Restore 547

Ustawienia ochrony 195

Ustawienia ochrony prywatności 21

Ustawienia sieciowe 775

Ustawienia usługi Active Protection w oprogramowaniu Cyber Backup Standard 898

Ustawienia zaawansowane 941

Ustawienia zabezpieczeń IPsec/IKE 813

Ustawienia zarządzania poprawkami w planie ochrony 1045

Usuwanie dostępu do połączenia z chmurą publiczną 598

Usuwanie dostępu do subskrypcji platformy Microsoft Azure 594

Usuwanie grupy 358

Usuwanie konfliktów między planami 228

Usuwanie kopii zapasowych 572

Usuwanie kopii zapasowych poza konsolą Cyber Protect 574

Usuwanie maszyny 727

Usuwanie niestandardowych serwerów DNS 826

Usuwanie obciążeń z konsoli Cyber Protect 330

Usuwanie obciążeń z planu zarządzania zdalnego 1092

Usuwanie organizacji Microsoft 365 653

Usuwanie planów z ulubionych 220

Usuwanie planu ochrony 228

Usuwanie poświadczeń 1099

Usuwanie wszystkich alertów 300

Uwaga dla użytkowników komputerów

© Acronis International GmbH, 2003-2024

Mac 534

Uwierzytelnianie dwuskładnikowe 19

Uzyskiwanie certyfikatu na potrzeby kopii zapasowych z danymi do analizy śledczej 500

Uzyskiwanie dostępu do usługi Cyber Protection 22

Uzyskiwanie dostępu do usuniętych kopii zapasowych w niezmiennym magazynie 1184

Uzyskiwanie identyfikatora i klucza tajnego aplikacji 647

Użytkownicy są wylogowani 460

Użytkownik jest bezczynny 459

Używanie funkcji Universal Restore 546

Używanie haseł ze znakami specjalnymi lub spacjami 133

Używanie magazynu dołączonego lokalnie 738

Używanie zmiennych 486

V

Virtuozzo 42

Virtuozzo Hybrid Infrastructure 43

VMware 33

W

W pakiecie Google Workspace 687

W programie 644

W programie Cyber Protection 687

W przypadku jakich obciążeń, agentów i lokalizacji kopii można wyświetlać wąskie gardła? 578

W razie błędu spróbuj ponownie 492, 561

W razie błędu tworzenia migawki maszyny wirtualnej spróbuj ponownie 493

W usłudze Microsoft 365 645

Wartości pola Czynność 385

Warunki rozpoczęcia 416, 457

Warunki uruchomienia zadania 526

Ważne wskazówki 467

Wbudowane plany monitorowania 214

Wbudowane plany ochrony 208

Wbudowane plany zarządzania zdalnego 216

Wdrażanie agenta dla oVirt (urządzenie wirtualne) 164

Wdrażanie agenta dla Scale Computing HC3 (urządzenie wirtualne) 150

Wdrażanie agenta dla Synology 170

Wdrażanie agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne) 155

Wdrażanie agenta dla VMware (urządzenie wirtualne) 146

Wdrażanie agentów ochrony przy użyciu zasad grupy 143

Wdrażanie funkcji odzyskiwania po awarii 786

Wdrażanie szablonu OVA 166

Wdrażanie szablonu OVF 147

Wdrażanie szablonu QCOW2 151, 159

Wdrażanie urządzeń wirtualnych 146

Wersja próbna rozwiązania Cyber Disaster Recovery Cloud 790

Wersje skryptu 409

Weryfikacja sumy kontrolnej 238

Weryfikowanie autentyczności pliku przy użyciu usługi Notary 552, 708

Wiązanie maszyn wirtualnych 739

© Acronis International GmbH, 2003-2024

Widżet inwentaryzacji oprogramowania 294

Widżet Sesje zdalne 296

Widżety alertów 276

Widżety dotyczące instalacji poprawek 291

Widżety dotyczące oceny luk w zabezpieczeniach 289

Widżety inwentaryzacji sprzętu 295

Widżety kondycji dysków 285

Widżety monitorów 1178

Widżety pakietu Endpoint Detection and Response (EDR) 279

Widżety usługi Advanced Data Loss Prevention na pulpicie nawigacyjnym Przegląd 951

Windows 430

Włącz docelową maszynę wirtualną po zakończeniu odzyskiwania 566

Włącz tworzenie pełnych kopii zapasowych z usługą VSS 529

Włączanie funkcji modułu Endpoint Detection and Response (EDR) 961

Włączanie funkcji Odzyskiwanie jednym kliknięciem 509

Włączanie i wyłączanie magazynu z geograficzną nadmiarowością 1185

Włączanie i wyłączanie połączenia site-to-site 823

Włączanie i wyłączanie zarządzania zaporą 919

Włączanie lub wyłączanie kontroli urządzeń 363

Włączanie lub wyłączanie planu ochrony 227

Włączanie lub wyłączanie powiadomień systemu operacyjnego i alertów usługi 366

Włączanie modułu Advanced Data Loss Prevention w planach ochrony 938

Włączanie niezmiennego magazynu 1183

Włączanie skanowania w celu inwentaryzacji oprogramowania 1061

Włączanie skanowania w celu inwentaryzacji sprzętu 1066

Włączanie trybu monitorowania dla modułu Endpoint Detection and Response (EDR) 1029

Wstępne konfigurowanie wielu połączeń sieciowych 776

Wstępnie zdefiniowane skrypty 765

Wybieranie baz danych SQL 603

Wybieranie całego komputera 429

Wybieranie danych do uwzględnienia w kopii zapasowej 429

Wybieranie danych programu Exchange Server 604

Wybieranie dysków lub woluminów 429

Wybieranie folderów publicznych 657

Wybieranie komponentów do zainstalowania 189

Wybieranie konfiguracji ESXi 436

Wybieranie miejsca docelowego 441

Wybieranie plików lub folderów 433

Wybieranie plików z Dysku Google 700

Wybieranie plików z Dysku udostępnionego 704

Wybieranie poziomu dzierżawcy 315

Wybieranie skrzynek pocztowych Gmail 696

Wybieranie skrzynek pocztowych Microsoft 365 650

Wybieranie skrzynek pocztowych programu Exchange Online 638

Wybieranie skrzynek pocztowych programu

© Acronis International GmbH, 2003-2024

Exchange Server 613

Wybieranie stanu systemu 436

Wybieranie zespołów 676

Wybierz dostawcę migawek 528

Wybór danych programu SharePoint Online 672

Wybór plików magazynu OneDrive 667

Wybór skrzynek pocztowych 656

Wydajność 563, 734

Wydajność i okno na utworzenie kopii zapasowej 513

Wykluczanie podklas urządzeń z kontroli dostępu 366

Wykluczanie poszczególnych urządzeń USB z kontroli dostępu 367

Wykluczanie procesów z kontroli dostępu 381

Wykluczenia 918

Wykluczenia adresów URL 914

Wykluczenia plików 561

Wykluczenia z ochrony 894

Wykonywanie automatycznego i ręcznego wykrywania 183

Wykonywanie automatycznego wykrywania komputerów na poziomie dzierżawcy-partnera 319

Wykonywanie czynności związanych ze sterowaniem na obciążeniach zarządzanych 1106

Wykonywanie migawek LVM 506

Wykonywanie powrotu po awarii 733

Wykonywanie powrotu po awarii na komputer fizyczny 854

Wykonywanie powrotu po awarii na maszynę wirtualną 849

Wykonywanie przełączenia awaryjnego 844

Wykonywanie ręcznego powrotu po awarii 857

Wykonywanie runbooka 873

Wykonywanie testowego przełączenia awaryjnego 839

Wykonywanie trwałego przełączenia awaryjnego 732

Wykres spalania dotyczący incydentów bezpieczeństwa 281

Wykryte komputery 278

Wykrywanie na podstawie taktyk 282

Wykrywanie procesów cryptominingu 886

Wyłączanie automatycznego harmonogramu zasobów rozproszonych (Distributed Resource Scheduler —DRS) dla agenta 146

Wyłączanie automatycznego przypisywania do agenta 741

Wyłączanie automatycznego testowego przełączania awaryjnego 843

Wyłączanie funkcji Odzyskiwanie jednym kliknięciem 511

Wyłączanie niezmiennego magazynu 1184

Wyłączanie wyszukiwania pełnotekstowego w przypadku kopii zapasowych usługi Gmail 712

Wymagane porty 170

Wymagane prawa użytkownika 614, 644, 687

Wymagane prawa użytkownika w przypadku tworzenia kopii zapasowych uwzględniających aplikacje 611

Wymagane role 170

Wymagane uprawnienia dla agenta dla VMware 744

Wymagania 555, 568

© Acronis International GmbH, 2003-2024

Wymagania dotyczące dostępu potrzebnego do tworzenia kopii zapasowych w chmurze publicznej 588

Wymagania dotyczące funkcji Kontrola konta użytkownika (UAC) 188

Wymagania dotyczące hasła 19

Wymagania dotyczące kont użytkowników 627

Wymagania dotyczące maszyn wirtualnych ESXi 602

Wymagania dotyczące maszyn wirtualnych Hyper-V 602

Wymagania dotyczące miejsca na dysku 543, 782

Wymagania dotyczące oprogramowania 23, 787, 961

Wymagania systemowe 808

Wymagania systemowe agenta 146, 150, 155, 164

Wymagania systemowe agentów 71

Wymagania urządzenia VPN 808

Wymagania wstępne 139, 143, 173, 175, 177, 179-181, 218-221, 315, 319, 389-390, 399, 410, 436, 512, 555, 601, 714, 725, 742, 811, 817, 823, 826, 834-835, 849, 854, 859, 1058, 1062-1063, 1065, 1067, 1070, 1083, 1091-1095, 1101, 1104-1106, 1108-1112, 1157, 1159-1160, 1163-1166, 1177

Wymazywanie danych z zarządzanego obciążenia 387

Wynik #CyberFit komputerów 391

Wynik #CyberFit według komputerów 283

Wyodrębnianie plików MSI, MST i CAB 101

Wyodrębnianie plików z lokalnych kopii zapasowych 555

Wyrażenie logiczne dla języka japońskiego 946

Wyrażenie logiczne używane w celu wykrywania zawartości 944, 946-947

Wyrażenie logiczne w przypadku wszystkich obsługiwanych języków z wyjątkiem japońskiego 946

Wyrejestrowywanie maszyn 136

Wysoka dostępność odzyskanej maszyny 752

Występujące luki w zabezpieczeniach 290

Wyszukiwanie pełnotekstowe 709

Wyszukiwanie w kopiach zapasowych z chmury do chmury 709

Wyszukiwanie zdarzeń 971

Wyświetlanie alertów z monitorowania dotyczących wybranego obciążenia 1175

Wyświetlanie alertów związanych z kontrolą urządzeń 369

Wyświetlanie danych z monitora 1177

Wyświetlanie dziennika alertów dotyczących monitorowania 1175

Wyświetlanie historii wykonania 873

Wyświetlanie i aktualizowanie lokalizacji kopii zapasowych w chmurze publicznej 586

Wyświetlanie incydentów, których skutków jeszcze nie zniwelowano 967

Wyświetlanie listy dostępnych poprawek 1051

Wyświetlanie lub zmienianie ustawień dostępu 365

Wyświetlanie maszyn wybranych klientów 317

Wyświetlanie sprzętu wybranego urządzenia 1070

Wyświetlanie statusu automatycznego testowego przełączania awaryjnego 843

Wyświetlanie statusu kopii zapasowej w kliencie vSphere 744

© Acronis International GmbH, 2003-2024

Wyświetlanie statusu sprawdzania poprawności kopii zapasowej 241

Wyświetlanie szczegółowych informacji na temat pozycji z białej listy 923

Wyświetlanie szczegółów wąskich gardeł 576

Wyświetlanie wyników inwentaryzacji oprogramowania wybranego urządzenia 1064

Z

Zaawansowana ochrona przed złośliwym oprogramowaniem 882

Zaawansowana opcja magazynu 442

Zaawansowany 917

Zabezpieczenia 1079

Zabezpieczenia na poziomie plików 562

Zadanie mieści się w przedziale czasu 461

Zalecenia 560

Zalecenia dotyczące dostępności usług Active Directory Domain Services 816

Zalecenia i kroki naprawcze 960

Zanim zaczniesz 63, 146, 150, 155, 164, 170

Zapisywanie pliku dziennika agenta 198

Zapisz informacje o systemie w razie niepowodzenia odzyskiwania z ponownym rozruchem 561

Zaplanuj skanowanie 890, 916

Zaplanuj według czasu 450

Zapobieganie nieuprawnionym dezinstalacjom lub modyfikacjom agentów 192

Zapoznawanie się z widokiem cybernetycznego łańcucha zabijania i jego dostosowywanie 989

Zarządzanie docelowymi obciążeniami w ramach planu 417

Zarządzanie dostępem do innych usług chmur publicznych 595

Zarządzanie dostępem do kont w chmurze publicznej 587

Zarządzanie dostępem do subskrypcji platformy Microsoft Azure 591

Zarządzanie incydentami na stronie Incydenty 959

Zarządzanie inwentaryzacją oprogramowania i sprzętu 1061

Zarządzanie izolacją sieci obciążenia 1010

Zarządzanie licencjami dla lokalnych serwerów zarządzania 206

Zarządzanie obciążeniami w konsoli Cyber Protect 313

Zarządzanie plikami poddanymi kwarantannie 920

Zarządzanie poprawkami 1044

Zarządzanie serwerami chmurowymi 862

Zarządzanie sieciami 818

Zarządzanie tokenami rejestracji 131

Zarządzanie tworzeniem kopii zapasowych oraz odzyskiwaniem obciążeń i plików 424

Zarządzanie ustawieniami połączenia point-to-site 828

Zarządzanie ustawieniami urządzenia VPN 822

Zarządzanie wykrytymi komputerami 190

Zarządzanie wykrytymi niechronionymi plikami 301

Zarządzanie zaporą 918

Zarządzanie zasilaniem maszyn wirtualnych 565, 734

Zarządzanie znalezionymi lukami w zabezpieczeniach 1042

© Acronis International GmbH, 2003-2024

Zasady działania konwersji regularnej na maszynę wirtualną 246

Zatrzymywanie przełączenia awaryjnego 732

Zatrzymywanie wykonywania runbooka 873

Zdalny dostęp VPN point-to-site 806

Zdarzenia funkcji Zapobieganie utracie danych 949

Zezwalanie na ruch DHCP przez połączenie L2 VPN 827

Zmiana identyfikatorów SID 565

Zmiana poświadczeń dostępu programu SQL Server lub Exchange Serwer 633

Zmiana rejestracji obciążenia 137

Zmienianie formatu kopii zapasowych na wersję 12 (TIBX) 488

Zmienianie hasła szyfrowania 1181

Zmienianie konfiguracji adresu IP 820

Zmienianie konta logowania na komputerach z systemem Windows 86

Zmienianie konta użytkownika dla agenta dla VMware 751

Zmienianie limitów usług komputerów 193

Zmienianie limitu czasu pulsu maszyny wirtualnej i sprawdzania poprawności zrzutu ekranu 240

Zmienianie portów używanych przez agenta ochrony 66

Zmienianie poświadczeń dostępu do usługi Microsoft 365 649

Zmienianie przypisania adresów IP 825

Zmienianie statusu skryptu 410

Zmienianie typu łączności na site-to-site 824

Zmienne alertów dotyczących monitorowania 1169

Znajdź ostatniego zalogowanego użytkownika 390

Znane problemy 714

Znane problemy i ograniczenia 957

© Acronis International GmbH, 2003-2024