



Acronis Backup & Recovery 11

Update 0

Podręcznik użytkownika

Dotyczy następujących wersji:

- ☒ Advanced Server
- ☒ Virtual Edition
- ☒ Advanced Server SBS Edition
- ☒ Advanced Workstation
- ☐ Server for Linux
- ☐ Server for Windows
- ☐ Workstation

Copyright © Acronis, Inc., 2000-2011. Wszelkie prawa zastrzeżone.

„Acronis” oraz „Acronis Secure Zone” są zastrzeżonymi znakami towarowymi firmy Acronis, Inc.

„Acronis Compute with Confidence”, „Acronis Startup Recovery Manager”, „Acronis Active Restore” i logo Acronis są znakami towarowymi firmy Acronis, Inc.

Linux jest zastrzeżonym znakiem towarowym Linusa Torvaldsa.

VMware i VMware Ready są znakami towarowymi lub zastrzeżonymi znakami towarowymi VMware, Inc. w Stanach Zjednoczonych i/lub innych jurysdykcjach.

Windows i MS-DOS są zastrzeżonymi znakami towarowymi firmy Microsoft Corporation.

Wszystkie inne wymienione znaki towarowe i prawa autorskie stanowią własność ich odpowiednich właścicieli.

Rozpowszechnianie niniejszego dokumentu w wersjach znacząco zmienionych jest zabronione bez wyraźnej zgody właściciela praw autorskich.

Rozpowszechnianie niniejszego lub podobnego opracowania w jakiegokolwiek postaci książkowej (papierowej) dla celów handlowych jest zabronione bez uprzedniej zgody właściciela praw autorskich.

DOKUMENTACJA ZOSTAJE DOSTARCZONA W TAKIM STANIE, W JAKIM JEST („TAK JAK JEST”) I WSZYSTKIE WARUNKI, OŚWIADCZENIA I DEKLARACJE WYRAŻNE LUB DOROZUMIANE, W TYM WSZELKIE GWARANCJE ZBYWALNOŚCI, PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB NIENARUSZANIA PRAW ZOSTAJĄ WYŁĄCZONE, Z WYJĄTKIEM ZAKRESU, W JAKIM TE WYŁĄCZENIA ZOSTANĄ UZNANE ZA NIEZGODNE Z PRAWEM.

Oprogramowanie lub Usługa może zawierać kod strony trzeciej. Warunki licencji takich kodów zamieszczono w pliku license.txt, znajdującym się w głównym katalogu instalacyjnym. Najnowsze informacje dotyczące kodów innych producentów zawartych w oprogramowaniu i/lub usłudze oraz dotyczące ich warunki licencji można znaleźć pod adresem <http://kb.acronis.com/content/7696>.

Spis treści

1	Wprowadzenie do programu Acronis Backup & Recovery 11	9
1.1	Co nowego w programie Acronis Backup & Recovery 11?	9
1.2	Acronis Backup & Recovery 11 — komponenty	12
1.2.1	Agent dla systemu Windows	12
1.2.2	Agent dla systemu Linux	13
1.2.3	Agent for VMware vSphere ESX(i)	14
1.2.4	Agent for Hyper-V	14
1.2.5	Komponenty do zarządzania scentralizowanego	14
1.2.6	Konsola zarządzania	16
1.2.7	Generator nośnika startowego	16
1.2.8	Program Acronis Wake-on-LAN Proxy	17
1.3	Obsługiwane systemy plików	17
1.4	Pomoc techniczna	17
2	Wprowadzenie	19
2.1	Używanie konsoli zarządzania	22
2.1.1	Panel „Nawigacja”	23
2.1.2	Obszar główny, widoki i strony czynności	25
2.1.3	Opcje konsoli	29
3	Opis programu Acronis Backup & Recovery 11	32
3.1	Właściciele i poświadczenia	32
3.2	Uprawnienia użytkownika na zarządzanym komputerze	33
3.3	Pełne, przyrostowe i różnicowe kopie zapasowe	34
3.4	Co zawiera kopia zapasowa dysku lub woluminu?	36
3.5	Informacje na temat woluminów dynamicznych i logicznych	36
3.5.1	Tworzenie kopii zapasowych woluminów dynamicznych i ich odzyskiwanie (system Windows)	36
3.5.2	Tworzenie kopii zapasowych i odzyskiwanie woluminów logicznych i urządzeń MD (system Linux)	39
3.6	Kompatybilność z programami szyfrującymi	45
3.7	Obsługa SNMP	46
4	Kopia zapasowa	48
4.1	Utwórz kopię zapasową	48
4.2	Tworzenie planu tworzenia kopii zapasowych	48
4.2.1	Wybieranie danych do uwzględnienia w kopii zapasowej	50
4.2.2	Poświadczenia dostępu do źródła	52
4.2.3	Wykluczenie plików źródłowych	52
4.2.4	Poświadczenia dostępu do lokalizacji archiwum	54
4.2.5	Schematy tworzenia kopii zapasowych	54
4.2.6	Wybór lokalizacji kopii zapasowej	65
4.2.7	Sprawdzanie poprawności archiwum	67
4.2.8	Poświadczenia planu tworzenia kopii zapasowych	68
4.2.9	Etykieta (zachowanie właściwości komputera w kopii zapasowej)	68
4.2.10	Dlaczego program wyświetla monit o hasło?	70
4.3	Uprozczone nazewnictwo plików kopii zapasowych	70
4.3.1	Przykłady użycia	71
4.3.2	Zmienna [DATE]	74
4.3.3	Podział kopii zapasowych i uproszczone nazewnictwo plików	74

4.4	Tworzenie harmonogramu	74
4.4.1	Harmonogram dzienny	76
4.4.2	Harmonogram tygodniowy	78
4.4.3	Harmonogram miesięczny	80
4.4.4	Po zdarzeniu zarejestrowanym w dzienniku systemu Windows	83
4.4.5	W przypadku alertu programu Acronis Drive Monitor	85
4.4.6	Zaawansowane ustawienia harmonogramu	85
4.4.7	Warunki	87
4.5	Replikacja i przechowywanie kopii zapasowych	90
4.5.1	Obsługiwane lokalizacje	92
4.5.2	Konfigurowanie replikacji kopii zapasowych	93
4.5.3	Konfigurowanie reguł przechowywania kopii zapasowych	93
4.5.4	Reguły przechowywania schematu niestandardowego	94
4.5.5	Czas braku aktywności replikacji/czyszczenia	96
4.5.6	Przykłady użycia	96
4.6	Konfigurowanie regularnej konwersji na maszynę wirtualną	99
4.6.1	Konfigurowanie harmonogramu konwersji	100
4.6.2	Wybieranie komputera, który przeprowadzi konwersję	100
4.6.3	Zasada działania zwykłej konwersji na maszynę wirtualną (VM)	101
4.7	Domyślne opcje tworzenia kopii zapasowej	102
4.7.1	Ustawienia dodatkowe	105
4.7.2	Ochrona archiwum	107
4.7.3	Katalogowanie kopii zapasowej	108
4.7.4	Wydajność tworzenia kopii zapasowej	108
4.7.5	Dzielenie kopii zapasowej	109
4.7.6	Stopień kompresji	110
4.7.7	Plan odzyskiwania po awarii (DRP)	111
4.7.8	Obsługa błędów	112
4.7.9	Śledzenie zdarzeń	112
4.7.10	Szybka przyrostowa/różnicowa kopia zapasowa	114
4.7.11	Migawka kopii zapasowej na poziomie pliku	114
4.7.12	Zabezpieczenia na poziomie plików	115
4.7.13	Wykonywanie migawek LVM	115
4.7.14	Komponenty na nośniku	116
4.7.15	Punkty zamontowania	117
4.7.16	Migawka wielowoluminowa	117
4.7.17	Powiadomienia	118
4.7.18	Polecenia poprzedzające/następujące	119
4.7.19	Polecenia poprzedzające rejestrowanie danych/następujące po nim	121
4.7.20	Czas braku aktywności replikacji/czyszczenia	123
4.7.21	Kopia zapasowa sektor po sektorze	124
4.7.22	Zarządzanie taśmami	124
4.7.23	Obsługa niepowodzenia zadania	125
4.7.24	Warunki uruchomienia zadania	126
4.7.25	Usługa kopiowania woluminów w tle	127
5	Odzyskiwanie	129
5.1	Tworzenie zadania odzyskiwania	130
5.1.1	Elementy do odzyskania	131
5.1.2	Poświadczenia dostępu do lokalizacji	135
5.1.3	Poświadczenia dostępu do miejsca docelowego	136
5.1.4	Lokalizacja odzyskiwania	136
5.1.5	Czas odzyskiwania	144
5.1.6	Poświadczenia zadania	145
5.2	Acronis Universal Restore	145

5.2.1	Uzyskiwanie narzędzia Universal Restore	145
5.2.2	Używanie funkcji Universal Restore.....	146
5.3	Odzyskiwanie systemów opartych na systemie BIOS w systemach opartych na technologii UEFI i na odwrót	149
5.3.1	Odzyskiwanie woluminów.....	149
5.3.2	Odzyskiwanie dysków	152
5.4	Acronis Active Restore.....	156
5.5	Jak przekonwertować kopię zapasową dysku na maszynę wirtualną	158
5.5.1	Wybór typu maszyny wirtualnej/serwera wirtualizacji.....	160
5.5.2	Ustawienia maszyn wirtualnych.....	160
5.6	Rozwiązywanie problemów z funkcjami startowymi dysku	161
5.6.1	Jak ponownie aktywować program GRUB i zmienić jego konfigurację	163
5.6.2	Moduły ładujące w systemie Windows.....	164
5.7	Domyślne opcje odzyskiwania	165
5.7.1	Ustawienia dodatkowe.....	166
5.7.2	Obsługa błędów.....	168
5.7.3	Śledzenie zdarzeń	168
5.7.4	Zabezpieczenia na poziomie plików.....	169
5.7.5	Punkty zamontowania	170
5.7.6	Powiadomienia.....	170
5.7.7	Polecenia poprzedzające/następujące	172
5.7.8	Priorytet odzyskiwania.....	173
6	Przechowywanie danych w kopiach zapasowych	175
6.1	Skarbce.....	175
6.1.1	Korzystanie ze skarbców.....	176
6.1.2	Skarbce centralne.....	177
6.1.3	Skarbce osobiste.....	185
6.2	Strefa Acronis Secure Zone	188
6.2.1	Tworzenie strefy Acronis Secure Zone	188
6.2.2	Zarządzanie strefą Acronis Secure Zone	190
6.3	Urządzenia taśmowe	191
6.3.1	Co to jest urządzenie taśmowe?	192
6.3.2	Omówienie obsługi urządzeń taśmowych	192
6.3.3	Rozpoczęcie pracy z urządzeniem taśmowym.....	195
6.3.4	Zarządzanie taśmami	200
6.3.5	Skarbce na taśmach	208
6.3.6	Przykłady użycia.....	209
6.4	Węzły magazynowania	212
6.4.1	Co to jest węzeł magazynowania?	213
6.4.2	Obsługiwane typy pamięci masowej	213
6.4.3	Operacje wykonywane przez węzły magazynowania	213
6.4.4	Rozpoczęcie pracy z węzłem magazynowania.....	214
6.4.5	Uprawnienia użytkownika w węźle magazynowania	215
6.4.6	Operacje na węzłach magazynowania	216
6.4.7	Deduplikacja	224
7	Operacje na archiwach i kopiach zapasowych	231
7.1	Sprawdzanie poprawności archiwów i kopii zapasowych	231
7.1.1	Wybór archiwum.....	232
7.1.2	Wybór kopii zapasowej.....	233
7.1.3	Wybór skarbca.....	233
7.1.4	Poświadczenia dostępu do źródła.....	233

7.1.5	Czas sprawdzania poprawności.....	234
7.1.6	Poświadczenia zadania	234
7.2	Eksportowanie archiwów i kopii zapasowych	235
7.2.1	Wybór archiwum.....	238
7.2.2	Wybór kopii zapasowej.....	238
7.2.3	Poświadczenia dostępu do źródła.....	238
7.2.4	Wybór miejsca docelowego	239
7.2.5	Poświadczenia dostępu do miejsca docelowego.....	240
7.3	Montowanie obrazu	241
7.3.1	Wybór archiwum.....	242
7.3.2	Wybór kopii zapasowej.....	243
7.3.3	Poświadczenia dostępu	243
7.3.4	Wybór woluminu	243
7.3.5	Zarządzanie zamontowanymi obrazami.....	244
7.4	Operacje dostępne w skarbcach.....	244
7.4.1	Operacje na archiwach	245
7.4.2	Operacje na kopiach zapasowych.....	245
7.4.3	Konwertowanie kopii zapasowej na pełną kopię zapasową.....	246
7.4.4	Usuwanie archiwów i kopii zapasowych	247
8	Nośnik startowy.....	248
8.1	Jak utworzyć nośnik startowy.....	249
8.1.1	Nośnik startowy oparty na systemie Linux.....	250
8.1.2	Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 1.x.....	255
8.1.3	Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 2.x lub 3.0	255
8.1.4	Generowanie środowiska Bart PE z wtyczką Acronis Plug-in z dystrybucji systemu Windows	257
8.2	Łączenie z komputerem uruchamianym z nośnika.....	257
8.3	Praca na nośniku startowym	258
8.3.1	Konfigurowanie trybu wyświetlania	258
8.3.2	Konfigurowanie urządzeń iSCSI i NDAS	259
8.4	Lista poleceń i narzędzi dostępnych na nośniku startowym opartym na systemie Linux	259
8.5	Acronis Startup Recovery Manager	261
8.6	Acronis PXE Server	261
8.6.1	Instalacja serwera Acronis PXE Server	262
8.6.2	Konfigurowanie komputera na potrzeby uruchamiania z serwera PXE	262
8.6.3	Praca w podsięciach.....	263
9	Zarządzanie dyskami	264
9.1	Obsługiwane systemy plików	264
9.2	Podstawowe środki ostrożności	265
9.3	Uruchamianie narzędzia Acronis Disk Director Lite.....	265
9.4	Wybieranie systemu operacyjnego do zarządzania dyskami	265
9.5	Widok „Zarządzanie dyskami”	266
9.6	Operacje na dyskach.....	266
9.6.1	Inicjowanie dysku	267
9.6.2	Klonowanie dysku podstawowego	267
9.6.3	Konwersja dysków: MBR na GPT	270
9.6.4	Konwersja dysku: GPT na MBR	270
9.6.5	Konwersja dysku: podstawowy na dynamiczny	271
9.6.6	Konwersja dysków: dynamiczne na podstawowe	272
9.6.7	Zmiana statusu dysku	273

9.7	Operacje w woluminach	273
9.7.1	Tworzenie woluminu	273
9.7.2	Usuń wolumin.....	277
9.7.3	Ustaw aktywny wolumin	278
9.7.4	Zmień literę woluminu.....	278
9.7.5	Zmień etykietę woluminu.....	279
9.7.6	Formatowanie woluminu	279
9.8	Operacje oczekujące	280
10	Administrowanie komputerem zarządzanym	282
10.1	Plany i zadania tworzenia kopii zapasowych	282
10.1.1	Czynności dotyczące planów i zadań tworzenia kopii zapasowych.....	282
10.1.2	Stany i statusy planów i zadań tworzenia kopii zapasowych	285
10.1.3	Eksportowanie i importowanie planów tworzenia kopii zapasowych	287
10.1.4	Wdrażanie planów tworzenia kopii zapasowych jako plików.....	290
10.1.5	Szczegóły planu tworzenia kopii zapasowych	292
10.1.6	Szczegóły zadania/działania	293
10.2	Dziennik	293
10.2.1	Czynności dotyczące wpisów dziennika	294
10.2.2	Szczegóły wpisu dziennika	295
10.3	Alerty	296
10.4	Zbieranie informacji o systemie.....	297
10.5	Dostosowywanie opcji komputera	297
10.5.1	Program jakości obsługi klienta.....	297
10.5.2	Alerty.....	297
10.5.3	Powiadomienia pocztą e-mail	298
10.5.4	Śledzenie zdarzeń	300
10.5.5	Reguły czyszczenia dziennika	302
10.5.6	Zarządzanie komputerem.....	302
10.5.7	Serwer proxy kopii zapasowej online	303
11	Zarządzanie scentralizowane	304
11.1	Opis zarządzania scentralizowanego	304
11.1.1	Podstawowe pojęcia	304
11.1.2	Uprawnienia zarządzania scentralizowanego.....	305
11.1.3	Komunikacja między komponentami programu Acronis Backup & Recovery 11.....	311
11.2	Tworzenie scentralizowanego planu tworzenia kopii zapasowych	315
11.2.1	Wybieranie danych do uwzględnienia w kopii zapasowej.....	315
11.2.2	Reguły wyboru plików i folderów	317
11.2.3	Reguły wyboru woluminów.....	319
11.2.4	Wybór lokalizacji kopii zapasowej.....	322
11.2.5	Poświadczenia scentralizowanego planu tworzenia kopii zapasowych	323
11.2.6	Co zrobić, jeśli na komputerze nie ma danych spełniających reguły wyboru.....	324
11.3	Administrowanie serwerem Acronis Backup & Recovery 11 Management Server	324
11.3.1	Pulpit nawigacyjny	324
11.3.2	Komputery z agentami.....	326
11.3.3	Maszyny wirtualne	339
11.3.4	Plany i zadania tworzenia kopii zapasowych.....	340
11.3.5	Węzły magazynowania	343
11.3.6	Licencje.....	343
11.3.7	Raporty.....	345
11.3.8	Alerty.....	351
11.3.9	Dziennik.....	352

11.3.10	Opcje serwera zarządzania	354
11.4	Konfigurowanie komponentów programu Acronis Backup & Recovery 11	360
11.4.1	Parametry konfigurowane przy użyciu szablonu administracyjnego.....	360
11.4.2	Parametry konfigurowane w graficznym interfejsie użytkownika	374
12	Słownik	375

1 Wprowadzenie do programu Acronis Backup & Recovery 11

1.1 Co nowego w programie Acronis Backup & Recovery 11?

Program Acronis Backup & Recovery 11 to kolejna wersja cieszącego się dużą popularnością programu Acronis Backup & Recovery 10, który zaoferował funkcje klasy korporacyjnej małym firmom po korzystnej cenie, w łatwym w obsłudze pakiecie.

Program Acronis Backup & Recovery 11 stanowi kontynuację trendu polegającego na rozszerzaniu możliwości tworzenia kopii zapasowych i odzyskiwania w środowiskach fizycznych, wirtualnych i przetwarzania w chmurze. Poniżej znajduje się podsumowanie nowych funkcji i usprawnień wprowadzonych w programie.

Wszystkie wersje

- **Uproszczona instalacja**

Nowy instalator upraszcza i usprawnia procedurę instalacji.

- **Ulepszona obsługa**

Przeprojektowany interfejs użytkownika programu umożliwia łatwiejsze, szybsze i bardziej intuicyjne wykonywanie każdej operacji.

- **Zaawansowana replikacja i przechowywanie kopii zapasowych (s. 90)**

Przechowywanie kopii zapasowych w wielu lokalizacjach (także w lokalizacjach poza siedzibą firmy) zapewniające nadmiarowość. Automatyczne przenoszenie lub kopiowanie kopii zapasowych do tańszego magazynu w innej lokalizacji. Konfigurowanie przedziału czasu replikacji w przypadku, gdy kopiowanie lub przenoszenie ma następować poza godzinami pracy.

- **Widok danych skarbów (s. 131)**

Możliwość wybierania danych ze skarbca przez przeglądanie archiwów i kopii zapasowych (w **Widoku archiwum**) lub danych uwzględnionych w kopiach zapasowych (w **Widoku danych**).

- **Powiadomienia o alertach (s. 296)**

Został wprowadzony nowy system alertów obejmujący zarówno zarządzanie lokalne, jak i scentralizowane. Możliwość wybrania alertów, które zamierza się obserwować. Konfigurowanie powiadomień pocztą e-mail o alertach poszczególnych typów.

- **Obsługa UEFI/GPT (s. 149)**

Pełna obsługa systemów opartych na technologii UEFI i dysków GPT. Odzyskiwanie systemów opartych na systemie BIOS w systemach opartych na technologii UEFI i na odwrót.

- **Obsługa dysków z sektorami 4 KB (s. 142)**

Podczas odzyskiwania dysków lub woluminów program automatycznie poprawia nieprawidłowo wyrównane woluminy — sytuację, w której klastry woluminów nie są wyrównane z sektorami dysku.

- **Wyrównywanie partycji (woluminów) (s. 142)**

Uzyskanie optymalnej wydajności dysków Solid State Drive (SSD) wymaga określonego wyrównania partycji. Wymagane wyrównanie jest ustawiane automatycznie podczas odzyskiwania, ale można je w razie potrzeby zmieniać ręcznie.

- **Automatyczne mapowanie dysków/woluminów** (s. 138)
Podczas odzyskiwania dysków lub woluminów program automatycznie w optymalny sposób mapuje wybrane dyski/woluminy na dyski docelowe.
- **Obsługa sprzętowych dostawców migawek** (s. 127)
Usługa kopiowania woluminów w tle (VSS) może do wykonywania migawek korzystać z dostawców sprzętowych.
- **Stosowanie narzędzia Acronis Universal Restore bez odzyskiwania** (s. 146)
Nośnik startowy pozwala na zastosowanie narzędzia Acronis Universal Restore w systemie operacyjnym bez odzyskiwania danych.
- **Obsługa mechanizmu LVM w systemie Linux** (s. 39)
Struktura LVM jest zapisywana w kopii zapasowej i może zostać odzyskana.
- **Narzędzie Acronis Universal Restore dla systemów Linux** (s. 148)
Odzyskiwanie systemów Linux na komputerze o innej konfiguracji sprzętowej.
- **Eksportowanie i importowanie planów tworzenia kopii zapasowych** (s. 287)
Eksportowanie planu tworzenia kopii zapasowych do pliku .xml i importowanie go na innym komputerze.
- **Wdrażanie planów tworzenia kopii zapasowych jako plików** (s. 290)
Eksportowanie planu tworzenia kopii zapasowych z jednego komputera i wdrażanie go w postaci pliku .xml na wielu innych komputerach.
- **Plan odzyskiwania po awarii** (s. 111)
Program umożliwia utworzenie planu odzyskiwania po awarii i wysłanie go pocztą e-mail natychmiast po utworzeniu kopii zapasowej. Plan zawiera szczegółowe instrukcje na temat sposobu odzyskiwania danych.
- **Konwertowanie kopii zapasowej na pełną kopię zapasową** (s. 246)
Konwertowanie kopii przyrostowej lub różnicowej na pełną.
- **Nowy wiersz poleceń**
Zapewnia automatyzację tworzenia kopii zapasowych i odzyskiwania. Obejmuje zdalne zarządzanie.
- **Automatyczne sprawdzanie dostępności aktualizacji**
Konsola zarządzania po każdym uruchomieniu automatycznie sprawdza dostępność aktualizacji i powiadamia o pojawieniu się nowszej wersji programu.

Wszystkie wersje zaawansowane

- **Wykaz danych i wyszukiwanie** (s. 134)
Scentralizowany wykaz danych umożliwia łatwe wyszukanie wymaganej wersji danych w centralnych skarbcach zarządzanych i wybranie jej do odzyskania.
- **Elastyczne wybieranie elementów danych do uwzględnienia w kopiach zapasowych** (s. 315)
Program umożliwia wybieranie poszczególnych elementów danych na każdym komputerze uwzględnionym w scentralizowanym planie tworzenia kopii zapasowych. Można również wybierać całe komputery lub grupy komputerów, a także korzystać z szablonów i zmiennych środowiskowych.
- **Lepsza deduplikacja** (s. 225)
Zwiększona wydajność deduplikacji: 2,5-5 razy szybciej. Kopie zapasowe plików są teraz deduplikowane na poziomie bloków, co radykalnie przyspiesza ich deduplikację w miejscu docelowym.

- **Lepsza obsługa taśm (s. 191)**
 Niezależność od Menedżera magazynu wymiennego systemu Windows. Zarządzanie nośnikami taśmowymi bezpośrednio z poziomu interfejsu użytkownika programu. Ulepszona obsługa bibliotek taśm. Możliwość tworzenia równoległych kopii zapasowych korzystających z wielu napędów taśmowych.
- **Uprawnienia dostępu do skarbów (s. 179)**
 Określanie kont użytkowników, którzy będą dysponowali prawami użytkowników i administratorów centralnych skarbów zarządzanych.
- **Zintegrowana instalacja zdalna**
 Serwer zarządzania umożliwia równoległe instalowanie agentów na wielu komputerach.
- **Zintegrowane zarządzanie licencjami (s. 343)**
 Serwer zarządzania obsługuje licencje samodzielnie. Nie ma potrzeby instalowania osobnego serwera licencji.
- **Instalacja bez serwera licencji (z wyjątkiem wersji Virtual Edition)**
 Podczas instalowania agenta zamiast serwera licencji można wprowadzić klucz licencyjny. Natychmiast po zarejestrowaniu na serwerze zarządzania klucz zostanie dodany do listy licencji obsługiwanych przez serwer.
- **Strona internetowa serwera zarządzania służąca do instalowania komponentów**
 Komponent serwera internetowego jest instalowany razem z serwerem zarządzania. Strona internetowa serwera zarządzania umożliwia pobieranie i instalowanie komponentów Acronis.

Virtual Edition

- **Przesyłanie kopii zapasowych za pomocą komponentu Agent for VMware vSphere ESX(i) (w systemie Windows)**
 Wersja agenta dla ESX(i) dla systemu Windows umożliwia przesyłanie kopii zapasowych z hosta ESX(i).
- **Obsługa klastrów Hyper-V**
 Tworzenie kopii zapasowych i odzyskiwanie maszyn wirtualnych w klastrach, w tym także znajdujących się na woluminach udostępnionych w klastrach systemu Windows 2008 R2.
- **Jednoczesne tworzenie kopii zapasowych maszyn wirtualnych**
 Agent może tworzyć równoległe kopie zapasowe nawet 10 maszyn wirtualnych. Dokładną ich liczbę określa użytkownik.
- **Tworzenie kopii zapasowych w magazynie dołączonym lokalnie**
 Po dodaniu do agenta dla ESX(i) (Virtual Appliance) specjalnego dysku wirtualnego można tworzyć kopie zapasowe bezpośrednio w tym magazynie, z pominięciem sieci LAN.
- **Elastyczna konfiguracja agentów do obsługi jednego lub wielu serwerów ESX(i)**
 Można chronić środowisko wirtualne za pomocą dowolnej liczby agentów, poczynając od jednego agenta dla wszystkich hostów, aż po jednego agenta na każdą z maszyn. Serwer zarządzania równomiernie rozdziela maszyny wirtualne pomiędzy agenty. Można również ręcznie powiązać agenty z poszczególnymi maszynami.
- **Automatyczne wdrażanie agentów**
 Wystarczy uwzględnić maszyny wirtualne ESX(i) w planie tworzenia kopii zapasowych. Agenty zostaną wdrożone i skonfigurowane w tle, jeśli zezwoli się na to podczas konfigurowania integracji z serwerem vCenter.
- **Konwersja przyrostowa na maszynę wirtualną (s. 101)**

Konwersja przyrostowej kopii zapasowej spowoduje aktualizację wstrzymanej maszyny zamiast tworzenia jej od podstaw.

1.2 Acronis Backup & Recovery 11 — komponenty

W tej sekcji znajduje się pełna lista komponentów programu Acronis Backup & Recovery 11 z krótkim opisem ich funkcji.

Program Acronis Backup & Recovery 11 zawiera następujące główne typy komponentów.

Komponenty dla komputera zarządzanego (agenty)

Są to aplikacje służące do tworzenia kopii zapasowych, odzyskiwania danych i wykonywania innych operacji na komputerach zarządzanych przy użyciu programu Acronis Backup & Recovery 11. Do wykonywania operacji na każdym komputerze zarządzanym agent potrzebuje licencji. Agenty mają wiele funkcji-dodatków oferujących dodatkowe możliwości, dlatego mogą wymagać dodatkowych licencji.

Komponenty do zarządzania scentralizowanego

Te komponenty, dostarczane z wersjami zaawansowanymi, umożliwiają zarządzanie scentralizowane. Korzystanie z tych komponentów nie wymaga licencji.

Konsola

Konsola ma graficzny interfejs użytkownika i umożliwia połączenie zdalne z agentami oraz innymi komponentami programu Acronis Backup & Recovery 11. Korzystanie z konsoli nie wymaga licencji.

Generator nośnika startowego

Za pomocą generatora nośnika startowego można tworzyć nośniki startowe, aby móc korzystać z agentów i innych narzędzi ratunkowych w środowisku ratunkowym.

Generator nośnika startowego nie wymaga licencji, jeśli jest instalowany razem z agentem. Wszystkie dodatki do agenta, jeśli są zainstalowane, będą dostępne w środowisku ratunkowym. Aby zainstalować generator nośnika na komputerze bez agenta, należy wprowadzić klucz licencyjny lub dysponować przynajmniej jedną licencją na serwerze licencji. Licencja może zostać udostępniona lub przypisana.

1.2.1 Agent dla systemu Windows

Agent ten umożliwia ochronę danych na poziomie dysków i na poziomie plików w systemie Windows.

Kopia zapasowa dysku

Ochrona danych na poziomie dysku polega na utworzeniu kopii zapasowej całego systemu plików dysku lub woluminu, wraz ze wszystkimi informacjami potrzebnymi do uruchomienia systemu operacyjnego, albo kopii zapasowej wszystkich sektorów dysku metodą „sektor po sektorze” (tryb „surowych” danych). Kopię zapasową danych dysku lub woluminu w postaci spakowanej określa się mianem kopii zapasowej dysku (woluminu) lub obrazem dysku (woluminu). Z takiej kopii zapasowej można odzyskać całe dyski lub woluminy, jak również poszczególne pliki lub foldery.

Kopia zapasowa plików

Ochrona danych na poziomie plików polega na utworzeniu kopii zapasowej plików i folderów znajdujących się na komputerze, na którym jest zainstalowany agent, lub w udziale sieciowym. Pliki można odzyskać w ich oryginalnej lokalizacji lub w innym miejscu. Odzyskać można wszystkie pliki i foldery znajdujące się w kopii zapasowej albo tylko wybrane z nich.

Inne operacje

Konwersja na maszynę wirtualną

Zamiast konwertować kopię zapasową dysku na plik dysku wirtualnego, co wymaga wykonania dodatkowych operacji przygotowujących dysk wirtualny do użytku, Agent dla systemu Windows wykonuje konwersję przez odzyskanie kopii zapasowej dysku na nową maszynę wirtualną jednego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) lub Red Hat Kernel-based Virtual Machine (KVM). Pliki w pełni skonfigurowanej i działającej maszyny są umieszczane w folderze wybranym przez użytkownika. Maszynę można uruchomić przy użyciu odpowiedniego oprogramowania do wirtualizacji lub przygotować pliki maszyny do dalszego użycia.

Zarządzanie dyskami

Agent dla systemu Windows zawiera wygodne narzędzie do zarządzania dyskami pod nazwą Acronis Disk Director Lite. Operacje zarządzania dyskami, takie jak klonowanie dysków, konwertowanie dysków, tworzenie, formatowanie i usuwanie woluminów, zmiana stylu partycjonowania dysku między MBR a GPT lub zmiana etykiety dysku, można wykonywać w systemie operacyjnym lub przy użyciu nośnika startowego.

Universal Restore

Na komputerze, na którym jest zainstalowany agent, dodatek Universal Restore umożliwia przywracanie danych na sprzęt o innej konfiguracji oraz utworzenie odpowiedniego nośnika startowego. Funkcja Universal Restore niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu operacyjnego, takimi jak kontrolery pamięci, płyta główna i chipset.

Deduplikacja

Ten dodatek umożliwia agentowi tworzenie kopii zapasowych w skarbcach deduplikacji zarządzanych przez węzeł magazynowania Acronis Backup & Recovery 11 Storage Node.

1.2.2 Agent dla systemu Linux

Agent ten umożliwia ochronę danych na poziomie dysków i na poziomie plików w systemie Linux.

Kopia zapasowa dysku

Ochrona danych na poziomie dysków polega na tworzeniu kopii zapasowej całego systemu plików dysku lub woluminu wraz ze wszystkimi informacjami potrzebnymi do uruchomienia systemu operacyjnego albo wszystkich sektorów dysku przy użyciu metody sektor po sektorze (tryb danych nieprzetworzonych). Kopia zapasowa dysku lub woluminu w postaci spakowanej to kopia zapasowa dysku (woluminu) lub obraz dysku (woluminu). Z takiej kopii zapasowej można odzyskać całe dyski lub woluminy, jak również poszczególne pliki lub foldery.

Kopia zapasowa plików

Ochrona danych na poziomie plików polega na tworzeniu kopii zapasowej plików i katalogów znajdujących się na komputerze, na którym jest zainstalowany agent, lub w udziale sieciowym udostępnionym przy użyciu protokołu smb lub nfs. Pliki można odzyskać do ich oryginalnej lokalizacji lub do innego miejsca. Odzyskać można wszystkie pliki i katalogi znajdujące się w kopii zapasowej albo tylko wybrane z nich.

Universal Restore

Na komputerze, na którym jest zainstalowany agent, dodatek Universal Restore umożliwia przywracanie danych na sprzęt o innej konfiguracji oraz utworzenie odpowiedniego nośnika startowego. Funkcja Universal Restore niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu operacyjnego, takimi jak kontrolery pamięci, płyta główna i chipset.

Deduplikacja

Ten dodatek umożliwia agentowi tworzenie kopii zapasowych w skarbcach deduplikacji zarządzanych przez węzeł magazynowania Acronis Backup & Recovery 11 Storage Node.

1.2.3 Agent for VMware vSphere ESX(i)

Komponent Acronis Backup & Recovery 11 Agent for VMware vSphere ESX(i) umożliwia tworzenie kopii zapasowych i odzyskiwanie maszyn wirtualnych ESX(i) bez konieczności instalowania agentów w systemach-gościach. Ta metoda tworzenia kopii zapasowych jest określana jako tworzenie kopii bez agenta lub na poziomie hiperwizora.

Agent występuje w dwóch wersjach:

- Agent for VMware vSphere ESX(i) (Virtual Appliance) może zostać zaimportowany lub wdrożony na hoście VMware ESX(i).
- Jeśli kopie zapasowe mają być przesyłane, komponent Agent for VMware vSphere ESX(i) (Windows) można zainstalować na komputerze z systemem Windows.

Acronis Backup & Recovery 11 Agent for VMware vSphere ESX(i) w dalszej części tego dokumentu występuje pod nazwą Agent for ESX(i).

1.2.4 Agent for Hyper-V

Komponent Acronis Backup & Recovery 11 Agent for Hyper-V chroni maszyny wirtualne znajdujące się na serwerze wirtualizacji Hyper-V ESX(i). Agent umożliwia tworzenie kopii zapasowych maszyn wirtualnych z hosta bez konieczności instalowania agentów na każdej maszynie wirtualnej. Agent można instalować w systemie Windows 2008 Server x64 (dowolnej wersji) lub Microsoft Hyper-V Server 2008.

1.2.5 Komponenty do zarządzania scentralizowanego

W tej sekcji znajduje się lista komponentów poszczególnych wersji programu Acronis Backup & Recovery 11 umożliwiającego zarządzanie scentralizowane. Na wszystkich komputerach, na których dane mają być chronione, oprócz wspomnianych komponentów należy zainstalować również agentów programu Acronis Backup & Recovery 11.

Serwer zarządzania

Serwer zarządzania Acronis Backup & Recovery 11 Management Server to centralny serwer odpowiedzialny za ochronę danych w sieci przedsiębiorstwa. Serwer zarządzania to dla administratora:

- jeden punkt wejścia do infrastruktury Acronis Backup & Recovery 11;
- łatwy sposób ochrony danych na wielu komputerach (s. 380) przy użyciu scentralizowanych planów tworzenia kopii zapasowych i możliwości ich grupowania;
- integracja z centrum VMware vCenter w celu wykrywania maszyn wirtualnych przeznaczonych do objęcia ochroną;
- funkcje monitorowania obejmujące całe przedsiębiorstwo;
- wbudowane zarządzanie licencjami;
- możliwość tworzenia skarbów centralnych (s. 385) do przechowywania archiwów kopii zapasowych (s. 376) przedsiębiorstwa;
- możliwość zarządzania węzłami magazynowania (s. 386);
- scentralizowany wykaz (s. 388) wszystkich danych przechowywanych w węzłach magazynowania.

Jeśli w sieci istnieje wiele serwerów zarządzania, działają one niezależnie, zarządzają innymi komputerami i zapisują archiwa w innych skarbcach centralnych.

Węzeł magazynowania

Węzeł magazynowania Acronis Backup & Recovery 11 Storage Node to serwer przeznaczony do optymalizacji wykorzystania różnych zasobów (takich jak pojemność firmowego magazynu, przepustowości sieci i obciążenia procesorów w komputerach zarządzanych) wymaganych do ochrony danych przedsiębiorstwa. Cel ten jest osiągany dzięki organizowaniu lokalizacji służących jako osobne magazyny dla archiwów kopii zapasowych przedsiębiorstwa (skarbcze zarządzane) i zarządzaniu nimi.

Najistotniejszą funkcją węzła magazynowania jest deduplikacja (s. 224) kopii zapasowych przechowywanych w jego skarbcach. Oznacza to, że identyczne dane zostaną uwzględnione w kopii zapasowej tylko raz. Minimalizuje to wykorzystanie sieci podczas tworzenia kopii zapasowej oraz zmniejsza ilość zajmowanego miejsca w archiwum.

Węzły magazynowania umożliwiają tworzenie wysoce skalowalnej i elastycznej (pod względem obsługi sprzętu) infrastruktury magazynu. Można skonfigurować do 50 węzłów magazynowania, a każdy z nich może zarządzać nawet 20 skarbcami.

Administrator obsługuje węzły magazynowania centralnie przy użyciu serwera zarządzania Acronis Backup & Recovery 11 Management Server (s. 15). Bezpośrednie połączenie konsoli z węzłem magazynowania nie jest możliwe.

Komponenty do instalacji zdalnej

Są to pliki instalacyjne komponentów Acronis wykorzystywane przez Kreator instalacji zdalnej. Program instalacyjny zapisuje je w domyślnej lokalizacji i zapisuje w rejestrze ścieżkę do tej lokalizacji. Dzięki temu komponenty są zawsze dostępne w Kreatorze instalacji zdalnej jako „zarejestrowane komponenty”.

Jak wyłączyć instalację komponentów

Jeśli w programie instalacyjnym zaznaczono pole wyboru **Łączenie z komputerami zdalnymi** lub **Centralne monitorowanie i konfigurowanie**, komponenty przeznaczone do instalacji zdalnej są domyślnie wybrane. Ponieważ pliki instalacyjne zajmują około 600 MB miejsca na dysku, czasem

warto uniemożliwić ich lokalne zapisywanie przy każdorazowym instalowaniu konsoli. Można na przykład wyodrębnić pliki instalacyjne w folderze udostępnionym. Będą one dostępne dla wszystkich konsoli zarządzania działających w sieci. W Kreatorze instalacji zdalnej należy w takim przypadku określić ścieżkę do udostępnionego folderu zamiast wyboru „zarejestrowanych komponentów”.

Aby uniemożliwić lokalne zapisywanie plików instalacyjnych, zaznacz pole wyboru **Chcę ręcznie wybrać komponenty Acronis** i wyczyść pole wyboru **Komponenty do instalacji zdalnej** w następnym oknie.

PXE Server

Serwer Acronis PXE Server umożliwia uruchamianie komputerów na komponentach startowych Acronis za pośrednictwem sieci.

Uruchomienie przez sieć:

- Eliminuje potrzebę lokalnej obecności technika w celu zainstalowania nośnika startowego (s. 381) w systemie, który ma zostać uruchomiony;
- W czasie operacji grupowych skraca czas potrzebny do uruchomienia wielu komputerów (w porównaniu z korzystaniem z fizycznego nośnika startowego).

Serwer licencji

Serwer umożliwiający zarządzanie licencjami produktów Acronis i instalowanie komponentów wymagających licencji.

Aby uzyskać więcej informacji na temat serwera licencji Acronis License Server, zobacz sekcję „Korzystanie z serwera licencji Acronis License Server (s. 343)”.

1.2.6 Konsola zarządzania

Konsola zarządzania Acronis Backup & Recovery 11 Management Console to narzędzie administracyjne umożliwiające zdalny lub lokalny dostęp do agentów Acronis Backup & Recovery 11, a w wersjach produktu z funkcją zarządzania scentralizowanego — do serwera zarządzania Acronis Backup & Recovery 11 Management Server.

Konsola jest dystrybuowana w dwóch wersjach: dla systemu Windows i systemu Linux. Mimo że obie wersje umożliwiają łączenie się z dowolnym agentem Acronis Backup & Recovery 11 i serwerem zarządzania Acronis Backup & Recovery 11 Management Server, zalecane jest korzystanie z konsoli dla systemu Windows (o ile wybór jest możliwy). Konsola instalowana w systemie Linux ma ograniczoną funkcjonalność:

- Zdalna instalacja komponentów Acronis Backup & Recovery 11 jest niedostępna.
- Funkcje związane z usługą Active Directory, takie jak przeglądanie usługi AD, są niedostępne.

1.2.7 Generator nośnika startowego

Generator Acronis Bootable Media Builder to specjalne narzędzie do tworzenia nośnika startowego (s. 381). Generator nośnika jest dostępny do zainstalowania w dwóch wersjach: dla systemu Windows i dla systemu Linux.

Generator nośnika dla systemu Windows umożliwia tworzenie nośnika startowego na podstawie środowiska preinstalacyjnego systemu Windows lub jądra systemu Linux. Generator nośnika instalowany w systemie Linux tworzy nośnik startowy na bazie jądra systemu Linux.

Dodatek Universal Restore (s. 13) umożliwia utworzenie nośnika startowego z funkcją przywracania na komputerze o innej konfiguracji sprzętowej. Funkcja Universal Restore niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu operacyjnego, takimi jak kontrolery pamięci, płyta główna i chipset.

Dodatek Deduplikacja (s. 13) umożliwia utworzenie nośnika startowego z funkcją tworzenia kopii zapasowych w skarbca deduplikacji. Dodatek ten można zainstalować w obu wersjach generatora nośnika.

1.2.8 Program Acronis Wake-on-LAN Proxy

Program Acronis Wake-on-LAN Proxy włącza wybudzanie serwera zarządzania Acronis Backup & Recovery 11 Management Server w celu tworzenia kopii zapasowych komputerów znajdujących się w innej podsieci. Program Acronis Wake-on-LAN Proxy należy zainstalować na dowolnym serwerze w podsieci obejmującej komputery, których kopię zapasową chcesz utworzyć.

1.3 Obsługiwane systemy plików

Program Acronis Backup & Recovery 11 umożliwia tworzenie kopii zapasowych i odzyskiwanie następujących systemów plików z poniższymi ograniczeniami:

- FAT16/32
- NTFS
- Ext2/Ext3/Ext4
- ReiserFS3 — nie można odzyskiwać poszczególnych plików z kopii zapasowych dysków znajdujących się w węźle magazynowania Acronis Backup & Recovery 11 Storage Node.
- ReiserFS4 — odzyskiwanie woluminu bez możliwości zmiany jego rozmiaru; nie można odzyskiwać poszczególnych plików z kopii zapasowych dysków znajdujących się w węźle magazynowania Acronis Backup & Recovery 11 Storage Node.
- XFS — odzyskiwanie woluminu bez możliwości zmiany jego rozmiaru; nie można odzyskiwać poszczególnych plików z kopii zapasowych dysków znajdujących się w węźle magazynowania Acronis Backup & Recovery 11 Storage Node.
- JFS — nie można odzyskiwać poszczególnych plików z kopii zapasowych dysków znajdujących się w węźle magazynowania Acronis Backup & Recovery 11 Storage Node.
- Plik wymiany (SWAP) systemu Linux.

Program Acronis Backup & Recovery 11 umożliwia tworzenie kopii zapasowych oraz odzyskiwanie uszkodzonych lub nieobsługiwanych systemów plików metodą „sektor po sektorze”.

1.4 Pomoc techniczna

Program pomocy technicznej i konserwacji

Jeśli będziesz potrzebować pomocy dotyczącej posiadanego produktu Acronis, przejdź na stronę <http://www.acronis.pl/support/>.

Aktualizacje produktów


Aby móc na bieżąco pobierać z naszej witryny internetowej najnowsze aktualizacje do wszystkich posiadanych produktów Acronis, zaloguj się na swoim koncie (<http://www.acronis.pl/my>) i zarejestruj produkty. Zobacz **Rejestrowanie produktów Acronis w witrynie internetowej**

(<http://kb.acronis.com/content/4834>) i **Podręcznik użytkownika witryny internetowej firmy Acronis** (<http://kb.acronis.com/content/8128>). Artykuły dostępne są w języku angielskim.

2 Wprowadzenie



Krok 1. Instalacja

 Poniższe krótkie instrukcje dotyczące instalacji umożliwiają szybkie rozpoczęcie pracy z programem. Aby uzyskać pełen opis procedur i sposobów instalacji, skorzystaj z Dokumentacji instalacji.

Przed instalacją należy sprawdzić, czy:

- Sprzęt spełnia wymagania systemowe.
- Dysponujesz kluczami licencyjnymi do wybranej wersji programu.
- Masz program instalacyjny. Można go pobrać z witryny internetowej firmy Acronis.

Procedura

Podczas wykonywania poniższych instrukcji można wybrać więcej niż jedną rolę komputera.

1. Zainstaluj serwer zarządzania, aby umożliwić zarządzanie wieloma komputerami.
 - a. Uruchom program instalacyjny i kliknij **Zainstaluj program Acronis Backup & Recovery 11**.
 - b. Po akceptacji warunków umowy licencyjnej zaznacz pole wyboru **Centralnie monitoruj i konfiguruj tworzenie kopii zapasowych komputerów fizycznych i maszyn wirtualnych**.
 - c. W oknie wyboru serwera licencji:
 - Pozostaw ustawienie domyślne: **Korzystaj z instalowanego serwera licencji wraz z serwerem zarządzania..**
 - Kliknij **Dodaj licencję**, a następnie wpisz klucze licencyjne lub zaimportuj je z pliku tekstowego.
 - d. Wykonaj instrukcje wyświetlane na ekranie.

Informacje szczegółowe. Aby możliwe było lokalne sterowanie serwerem zarządzania, zostanie zainstalowana także konsola.

2. Zainstaluj agenta na każdym komputerze, którego kopię zapasową chcesz utworzyć.
 - a. Uruchom program instalacyjny i kliknij **Zainstaluj program Acronis Backup & Recovery 11**.
 - b. Po akceptacji warunków umowy licencyjnej zaznacz pole wyboru **Utwórz kopię zapasową danych tego komputera**.
 - c. Kliknij **Pobierz klucze licencyjne z serwera licencji** i wprowadź nazwę lub adres IP wcześniej zainstalowanego serwera zarządzania.
 - d. Gdy pojawi się stosowny monit, zarejestruj komputer w serwerze zarządzania.
 - e. Wykonaj instrukcje wyświetlane na ekranie.

Informacje szczegółowe. Konsola będzie także zainstalowana na każdym komputerze.


3. [Opcjonalnie] Zainstaluj węzeł magazynowania na komputerze, który będzie służył jako magazyn kopii zapasowych innych komputerów.
 - a. Uruchom program instalacyjny i kliknij **Zainstaluj program Acronis Backup & Recovery 11**.
 - b. Po akceptacji warunków umowy licencyjnej zaznacz pole wyboru **Przechowywanie kopii zapasowych innych komputerów na tym komputerze**.
 - c. Gdy pojawi się stosowny monit, zarejestruj węzeł magazynowania w serwerze zarządzania.
 - d. Wykonaj instrukcje wyświetlane na ekranie.

4. [Opcjonalnie] Zainstaluj konsolę na preferowanym komputerze pod warunkiem, że komputer ten nie jest serwerem zarządzania i nie jest na nim zainstalowany agent.
 - a. Uruchom program instalacyjny i kliknij **Zainstaluj program Acronis Backup & Recovery 11**.
 - b. Po akceptacji warunków umowy licencyjnej zaznacz pole wyboru **Połącz z komputerem zdalnym**.
 - c. Wykonaj instrukcje wyświetlane na ekranie.



Krok 2. Uruchamianie

Uruchom konsolę Acronis Backup & Recovery 11 Management Console.

- W systemie **Windows** Uruchom konsolę, wybierając  **Acronis Backup & Recovery 11** w menu **Start**.
- W systemie **Linux** Zaloguj się jako root lub jako zwykły użytkownik, a następnie przełącz się na wymaganego użytkownika. Uruchom konsolę za pomocą polecenia

```
/usr/sbin/acronis_console
```





Aby zapoznać się z elementami graficznego interfejsu użytkownika, zobacz „Korzystanie z konsoli zarządzania” (s. 22).



Krok 3. Nośnik startowy

W celu przywrócenia systemu operacyjnego, którego nie da się uruchomić lub wdrożenia systemu operacyjnego na pustym dysku twardym należy utworzyć nośnik startowy.

1. Wybierz w menu  **Narzędzia** >  **Utwórz nośnik startowy**.
2. Kliknij **Dalej** w oknie powitalnym. Kontynuuj klikanie **Dalej** aż do pojawienia się listy komponentów.
3. Postępuj zgodnie z opisem w „Nośnik startowy oparty na systemie Linux” (s. 250).



Krok 4. Połączenie

Podłącz konsolę do komputera zarządzanego lub do serwera zarządzania.

Na pierwszej stronie konsoli kliknij jedną następujących opcji:



Zarządzaj tym komputerem

Jeśli agent jest zainstalowany na tym samym komputerze co konsola.



Zarządzaj komputerem zdalnym

Jeśli agent jest zainstalowany na komputerze zdalnym.



Podłącz do serwera zarządzania

Aby zarządzać wieloma komputerami fizycznymi i maszynami wirtualnymi.



Krok 5. Kopia zapasowa



Utwórz kopię zapasową (s. 48) (opcja jest niedostępna, jeśli konsola jest podłączona do serwera zarządzania)

Kliknij **Utwórz kopię zapasową**, aby w kilku prostych krokach utworzyć jednorazową kopię zapasową. Proces tworzenia kopii zapasowej rozpocznie się natychmiast po wykonaniu wymaganych kroków.

Aby zapisać kopię komputera do pliku:

W oknie **Miejsce docelowe kopii zapasowej** kliknij **Lokalizacja** i wybierz lokalizację do zapisania kopii zapasowej. Kliknij **OK**, aby zatwierdzić wybór. Kliknij **OK** u dołu okna, aby rozpocząć tworzenie kopii zapasowej.

Wskazówka. Przy użyciu nośnika startowego można wykonywać kopie zapasowe w trybie offline („zimne”) w taki sam sposób, jak w systemie operacyjnym.



Utwórz plan tworzenia kopii zapasowych (s. 48)

Utwórz plan tworzenia kopii zapasowych, jeśli istnieje potrzeba stosowania długotrwałej strategii tworzenia kopii zapasowych, która zawiera schematy kopii zapasowych, harmonogramy i warunki, okresowe usuwanie kopii bezpieczeństwa lub przenoszenie kopii zapasowych do innych lokalizacji.

Uwagi dla użytkowników wersji Advanced: Podczas tworzenia planu tworzenia kopii zapasowych w serwerze zarządzania można:

- wybrać całe komputery lub grupy komputerów;
- wybrać różne elementy na każdym komputerze;
- używać zasad wyboru w celu wybrania tych samych elementów na różnych komputerach.

W ten sposób utworzysz scentralizowany plan tworzenia kopii zapasowych przeznaczony do wdrożenia na wybranych komputerach. Aby uzyskać więcej informacji, zobacz „Tworzenie scentralizowanego planu tworzenia kopii zapasowych” (s. 315).



Krok 6. Odzyskiwanie



Odzyskiwanie (s. 130)

Aby odzyskać dane, należy wybrać dane z kopii zapasowej oraz lokalizację, do której dane zostaną odzyskane. W rezultacie powstanie zadanie odzyskiwania.

Odzyskanie dysku lub woluminu do woluminu zablokowanego przez system operacyjny wymaga ponownego uruchomienia komputera. Po zakończeniu procesu odzyskany system operacyjny automatycznie przechodzi w tryb online.





Jeśli rozruch komputera kończy się niepowodzeniem lub system trzeba odzyskać całkowicie od podstaw, należy uruchomić komputer przy użyciu nośnika startowego i skonfigurować operację odzyskiwania w taki sam sposób jak zadanie odzyskiwania.

Uwagi dla użytkowników wersji Advanced: Podczas używania nośnika startowego nie można sterować operacjami przez serwer zarządzania. Jednak możliwe jest odłączenie konsoli od serwera i podłączenie jej do komputera uruchomionego przy użyciu nośnika startowego.









Krok 7. Zarządzanie

Panel **Nawigacja** (z lewej strony w oknie konsoli) umożliwia przeglądanie widoków programów używanych w różnych celach administracyjnych.

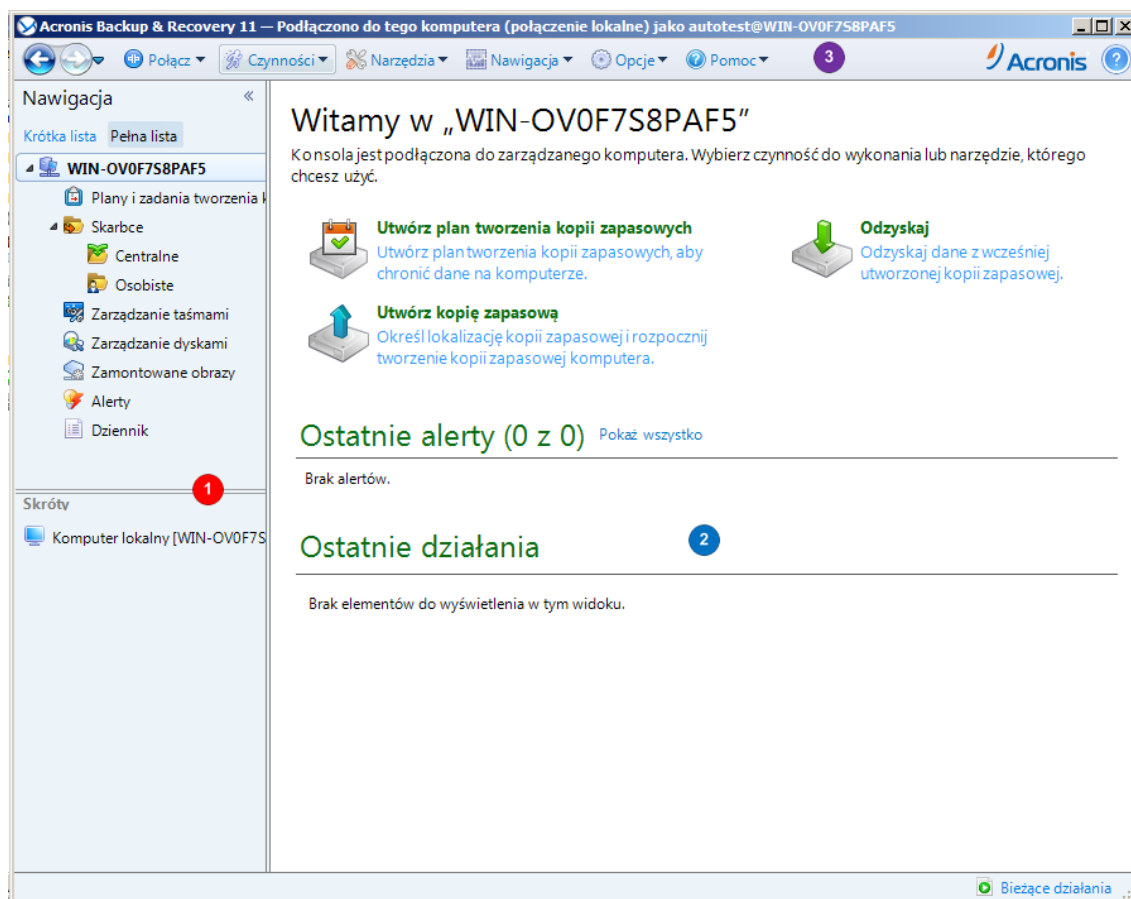
- Użyj widoku  **Plany i zadania tworzenia kopii zapasowych** do zarządzania planami i zadaniami tworzenia kopii zapasowych takich jak: uruchom, edytuj, zatrzymaj i usuń, oraz do przeglądania ich stanu oraz postępu operacji.
- Użyj widoku  **Alerty** do szybkiego rozpoznania i rozwiązywania problemów.
- Użyj widoku  **Dziennik**, aby przeglądać dziennik operacji.
- Lokalizacja, w której przechowywane są archiwa kopii zapasowych, nosi nazwę skarbca (s. 385). Przejdź do widoku  **Skarbce** (s. 175), aby wyświetlić informacje o skarbcach. Przejdź dalej do danego skarbcza, aby wyświetlić kopie zapasowe wraz z ich zawartością. Można w tym miejscu wybrać dane do odzyskania oraz wykonać ręczne operacje na kopiach zapasowych (montowanie, sprawdzanie poprawności, usuwanie).

Administrowanie serwerem zarządzania

- Użyj widoku  **Komputery z agentami**, aby zarządzać komputerami zarejestrowanymi w serwerze zarządzania. W celu efektywnej pracy z dużą liczbą komputerów można je organizować w grupy (s. 326).
- Użyj widoku  **Maszyny wirtualne** (s. 339), aby zarządzać obsługiwanymi środowiskami wirtualizacji.
- W przypadku wybrania opcji przechowywania wszystkich archiwów kopii zapasowych w jednej lub kilku lokalizacjach sieciowych należy utworzyć w tych lokalizacjach skarbcze centralne. Po utworzeniu skarbcza można przeglądać jego zawartość i zarządzać nią, wybierając  **Skarbce >  Centralne >  „Nazwa skarbcza”** w panelu **Nawigacja**. Skrót do skarbcza zostanie wdrożony na wszystkich zarejestrowanych komputerach. Skarbiec można wskazać jako miejsce docelowe kopii zapasowych w dowolnym planie tworzenia kopii zapasowych zdefiniowanym przez siebie lub przez użytkowników zarejestrowanych komputerów.
- Utwórz scentralizowane skarbcze zarządzane w węźle magazynowania (s. 214), aby móc:
 - Przeszukiwać  **Wykaz danych** (s. 134) we wszystkich skarbcach zarządzanych w celu znalezienia wymaganej wersji danych zapisanych w kopii zapasowej.
 - Tworzyć kopie zapasowe wielu komputerów na urządzeniach taśmowych (s. 191) podłączonych do węzła magazynowania.
 - Stosować deduplikację (s. 224) w celu minimalizacji zajętej przez dane przestrzeni magazynu oraz w celu zmniejszenia obciążenia sieci podczas trwania operacji tworzenia kopii zapasowej.

2.1 Używanie konsoli zarządzania

Po podłączeniu konsoli do komputera zarządzanego (s. 380) lub serwera zarządzania (s. 384) w jej obszarze roboczym (w menu, obszarze głównym z ekranem **Witamy** lub panelu **Nawigacja**) pojawią się odpowiednie elementy umożliwiające wykonywanie operacji przy użyciu agenta lub przy użyciu serwera.



Konsola zarządzania Acronis Backup & Recovery 11 Management Console — ekran Witamy

Główne elementy obszaru roboczego konsoli

	Nazwa	Opis
1	Panel Nawigacja	Zawiera drzewo Nawigacja oraz pasek Skróty . Umożliwia przechodzenie do poszczególnych widoków. Aby uzyskać szczegółowe informacje, zobacz Panel Nawigacja (s. 23).
2	Obszar główny	Umożliwia konfigurowanie i monitorowanie operacji tworzenia kopii zapasowych, odzyskiwania i innych. W obszarze głównym wyświetlane są różne widoki i strony czynności (s. 25), w zależności od elementów wybranych w menu lub drzewie Nawigacja .
3	Pasek menu	Znajduje się u góry okna programu. Umożliwia wykonywanie większości operacji dostępnych w programie Acronis Backup & Recovery 11. Elementy menu zmieniają się dynamicznie w zależności od elementu wybranego w drzewie Nawigacja i w obszarze głównym.

2.1.1 Panel „Nawigacja”

W panelu nawigacji znajduje się drzewo **Nawigacja** i pasek **Skróty**.





Drzewo nawigacji

Drzewo **Nawigacja** umożliwia przechodzenie między widokami programu. Dostępne widoki zależą od tego, czy konsola jest podłączona do zarządzanego komputera czy do serwera zarządzania. W obu przypadkach można wybierać między wyświetlaniem zestawu widoków w trybie **Pełna lista** lub **Krótką listą**. **Krótką listą** obejmuje najczęściej używane widoki z **Pełnej listy**.





Widoki dotyczące komputera zarządzanego

Po połączeniu konsoli z komputerem zarządzanym w drzewie nawigacji będą dostępne następujące widoki.

Krótką listą zawiera następujące elementy

-  **[Nazwa komputera]**. Podstawowy poziom drzewa, zwany również ekranem **powitalnym**. Jest w nim wyświetlana nazwa komputera, do którego jest aktualnie podłączona konsola. Widok ten umożliwia szybki dostęp do głównych operacji dostępnych na komputerze zarządzanym.
 -  **Plany i zadania tworzenia kopii zapasowych**. Ten widok służy do zarządzania planami i zadaniami tworzenia kopii zapasowych na komputerze zarządzanym: uruchamiania, edycji, zatrzymywania i usuwania planów oraz zadań, a także wyświetlania postępu ich realizacji.
 -  **Skarbcze**. Ten widok służy do zarządzania skarbami osobistymi i przechowywanymi w nich archiwami, dodawania nowych skarbców, zmiany nazw i usuwania istniejących skarbców, sprawdzania poprawności skarbców, przeglądania zawartości kopii zapasowych itd. Jeśli komputer jest zarejestrowany na serwerze zarządzania, możliwe jest przeglądanie skarbców centralnych i wykonywanie na archiwach operacji, do których ma się odpowiednie uprawnienia.
 -  **Alerty**. Ten widok służy do zapoznawania się z komunikatami ostrzegawczymi dotyczącymi zarządzanego komputera.






Pełną listą zawiera dodatkowo następujące elementy

-  **Zarządzanie taśmami**. Ten widok służy do wykonywania operacji na taśmach.
-  **Zarządzanie dyskami**. Ten widok służy do wykonywania operacji na dyskach twardych komputera.
-  **Dziennik**. Ten widok służy do analizowania informacji na temat operacji wykonywanych przez program na komputerze zarządzanym.
-  **Zamontowane obrazy**. Ten węzeł jest wyświetlany, gdy został zamontowany przynajmniej jeden wolumin. Widok ten służy do zarządzania zamontowanymi obrazami.


Widoki dotyczące serwera zarządzania

Po połączeniu konsoli z serwerem zarządzania w drzewie nawigacji będą dostępne następujące widoki.








Krótką listą zawiera następujące elementy

-  **[Nazwa serwera zarządzania]**. Podstawowy poziom drzewa, zwany również ekranem **powitalnym**. Jest w nim wyświetlana nazwa serwera zarządzania, do którego jest aktualnie podłączona konsola. Widok ten umożliwia szybki dostęp do głównych operacji dostępnych na serwerze zarządzania.
 -  **Pulpit nawigacyjny**. Ten widok służy do szybkiej oceny, czy dane na komputerach zarejestrowanych na serwerze zarządzania są skutecznie chronione.
 -  **Komputery z agentami**. Ten widok służy do zarządzania komputerami zarejestrowanymi na serwerze zarządzania.
 -  **Plany i zadania tworzenia kopii zapasowych**. Ten widok służy do zarządzania scentralizowanymi planami i zadaniami tworzenia kopii zapasowych na serwerze zarządzania.
 -  **Skarbcze**. Ten widok służy do zarządzania skarbami centralnymi i przechowywanymi w nich archiwami — tworzenia nowych skarbców zarządzanych, zmieniania nazw istniejących

skarbców i usuwania ich, przypisywania użytkowników i administratorów skarbców, wykonywania operacji na archiwach i kopiach zapasowych.

-  **Alerty.** Ten widok służy do zapoznawania się z komunikatami ostrzegawczymi dotyczącymi serwera zarządzania i wszystkich zarejestrowanych komputerów.

Pełna lista zawiera dodatkowo następujące elementy

-  **Wykaz danych.** Ten widok służy do szybkiego wyszukiwania wymaganej wersji danych w kopiach zapasowych w centralnych skarbcach zarządzanych.
-  **Maszyny wirtualne.** Ten widok służy do zarządzania obsługiwanymi środowiskami wirtualizacji.
-  **Węzły magazynowania.** Ten widok służy do zarządzania węzłami magazynowania. Po dodaniu węzła magazynowania można utworzyć skarbcę centralne zarządzane przez węzeł.
-  **Zarządzanie taśmami.** Ten widok służy do wykonywania operacji na taśmach.
-  **Licencje.** Ten widok służy do zarządzania licencjami.
-  **Raporty.** Ten widok służy do generowania raportów.
-  **Dziennik.** Ten widok służy do zapoznawania się z historią scentralizowanych operacji zarządzania, a także historią operacji zarejestrowanych w lokalnych dziennikach komputerów zarejestrowanych i węzłów magazynowania.

Pasek skrótów

Pasek **Skróty** znajduje się pod drzewem nawigacji. Umożliwia szybkie i wygodne tworzenie połączeń z żądanymi komputerami przez dodawanie skrótów do tych komputerów.



Aby dodać skrót do komputera

1. Podłącz konsolę do komputera zarządzanego.
2. W drzewie nawigacji kliknij prawym przyciskiem myszy nazwę komputera (element na podstawowym poziomie drzewa nawigacji), a następnie wybierz **Utwórz skrót**.

Jeśli konsola i agent są zainstalowane na tym samym komputerze, skrót do tego komputera zostanie dodany do paska skrótów automatycznie jako **Komputer lokalny [nazwa komputera]**.

Operacje na panelu

Rozwijanie/minimalizowanie paneli

Domyślnie panel **Nawigacja** jest rozwinięty. Czasem trzeba zminimalizować panel w celu zwolnienia miejsca w obszarze roboczym. W tym celu kliknij przycisk z pagonem (). Panel zostanie zminimalizowany, a pagon zmieni kierunek (). Kliknij go ponownie, aby rozwinąć panel.

Zmiana rozmiaru paneli

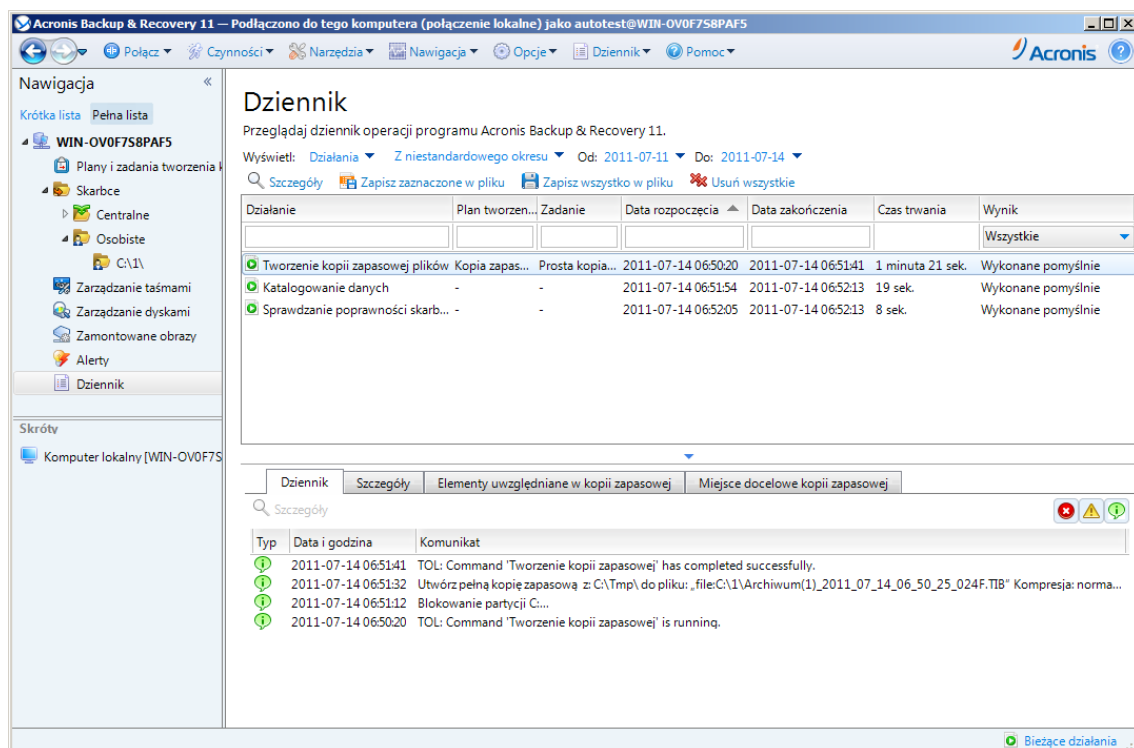
1. Wskaż obramowanie panelu.
2. Po zmianie wskaźnika na strzałkę dwukierunkową przeciągnij wskaźnik, aby przenieść obramowanie.

2.1.2 Obszar główny, widoki i strony czynności

Obszar główny to podstawowe miejsce pracy z konsolą. W tym miejscu można tworzyć i modyfikować plany tworzenia kopii zapasowych i zadania odzyskiwania oraz zarządzać nimi, a także wykonywać inne operacje. W obszarze głównym wyświetlane są różne widoki i strony czynności, w zależności od elementów wybranych w menu lub w drzewie **Nawigacja**.

Widoki

Widok pojawia się w obszarze głównym po kliknięciu dowolnego elementu w drzewie **Nawigacja** w panelu Nawigacja (s. 23).



Widok „Dziennik”

Typowy sposób pracy z widokami

Zwykle każdy widok zawiera tabelę elementów, pasek narzędzi tabeli z przyciskami oraz panel **Informacje**.

- Aby w tabeli wyszukać żądany element, użyj funkcji filtrowania i sortowania (s. 26).
- Wybierz żądany element w tabeli.
- W panelu Informacje (domyślnie zwinięty) przejrzyj szczegóły dotyczące elementu. Aby go rozwinąć, kliknij symbol strzałki (▲).
- Wykonaj czynności na wybranym elemencie. Te same czynności na wybranych elementach można wykonać na kilka sposobów:
 - Klikając przyciski na pasku narzędzi tabeli.
 - Wybierając elementy w menu **Czynności**.
 - Klikając element prawym przyciskiem myszy i wybierając operację w menu kontekstowym.

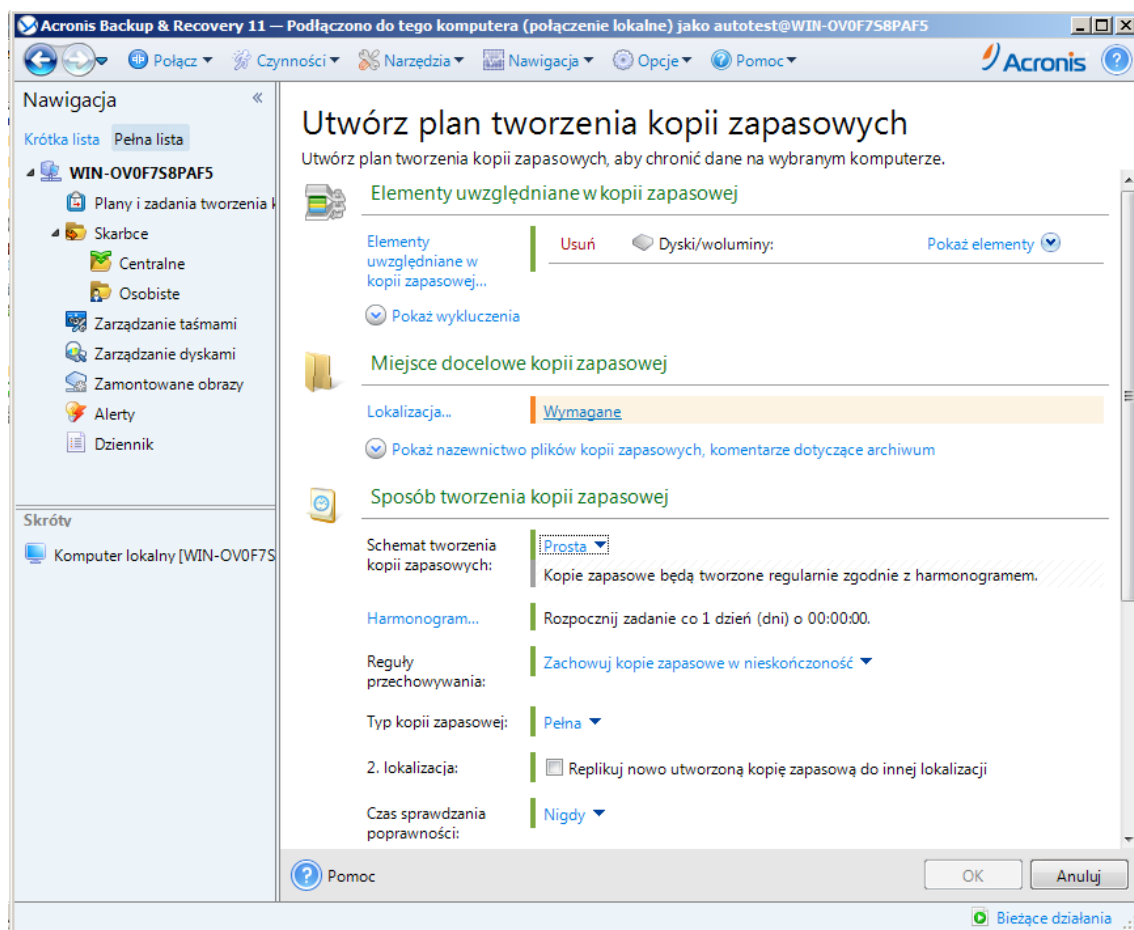
Sortowanie, filtrowanie i konfigurowanie elementów tabeli

Poniżej przedstawiono wskazówki dotyczące sortowania, filtrowania i konfigurowania elementów tabeli w dowolnym widoku.

Zadanie	Czynności
Sortowanie elementów według dowolnej kolumny	Kliknij nagłówek kolumny, aby posortować elementy w porządku rosnącym. Kliknij nagłówek ponownie, aby posortować elementy w porządku malejącym.
Filtrowanie elementów według wstępnie zdefiniowanej wartości kolumny	W polu pod odpowiednim nagłówkiem kolumny wybierz żądaną wartość z listy rozwijanej.
Filtrowanie elementów według wprowadzonej wartości	W polu pod odpowiednim nagłówkiem kolumny wpisz wartość. Zostanie wyświetlona lista wartości, które całkowicie lub częściowo odpowiadają wprowadzonej wartości.
Filtrowanie elementów według wstępnie zdefiniowanych parametrów	W zależności od widoku elementy tabeli można filtrować według pewnych wstępnie zdefiniowanych parametrów. Aby tego dokonać, klikaj odpowiednie przyciski lub łącza w górnej części tabeli. Na przykład: <ul style="list-style-type: none">W widoku Dziennik możesz filtrować wpisy zdarzeń, klikając przyciski powiązane z wynikiem: Wykonane pomyślnie, Wykonane pomyślnie z ostrzeżeniami lub Zakończone niepowodzeniem.W widoku Dziennik parametrem domyślnym jest godzina rozpoczęcia działania, natomiast trzy wstępnie zdefiniowane ustawienia do filtrowania działań według tego parametru (Wszystkie dostępne, Z ostatnich 3 miesięcy oraz Z niestandardowego okresu) znajdują się w górnej części widoku Dziennik.
Wyświetlanie lub ukrywanie kolumn tabeli	Domyślnie w każdej tabeli wyświetlana jest stała liczba kolumn, a pozostałe są ukryte. W razie potrzeby można ukryć wyświetlane kolumny i wyświetlić kolumny ukryte. Aby wyświetlić lub ukryć kolumny <ol style="list-style-type: none">Kliknij prawym przyciskiem myszy dowolny nagłówek kolumny, aby wyświetlić menu kontekstowe.Kliknij elementy, które chcesz wyświetlić/ukryć.

Strony czynności

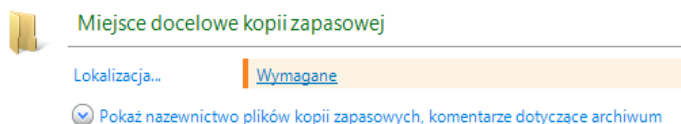
Strona czynności pojawia się w obszarze głównym po kliknięciu dowolnej czynności dostępnej w menu **Czynności**. Strona zawiera listę kroków, które należy wykonać, aby utworzyć i uruchomić dowolne zadanie lub plan tworzenia kopii zapasowych.



Strona czynności — Utwórz plan tworzenia kopii zapasowych

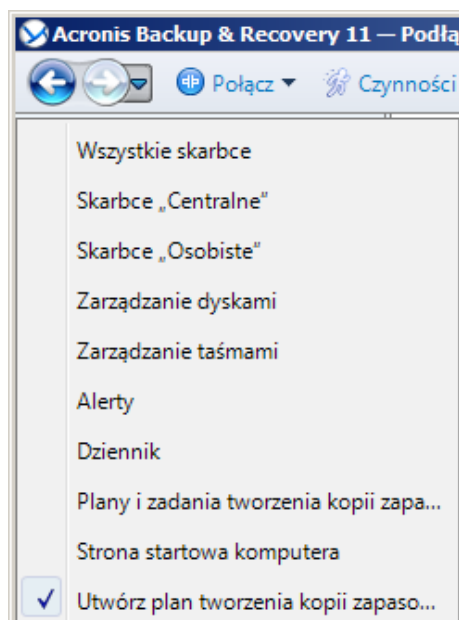
Korzystanie z formantów i określanie ustawień

Za pomocą aktywnych formantów określ ustawienia i parametry planu tworzenia kopii zapasowych lub zadania odzyskiwania. Domyślnie pewne pola, takie jak poświadczenia, opcje, komentarze i niektóre inne, są ukryte. Większość ustawień konfiguruje się, klikając odpowiednie łącza **Pokaż**. Inne ustawienia należy wybrać na liście rozwijanej lub wpisać ich wartości w polach na stronie.



Strona czynności — elementy sterujące

Program Acronis Backup & Recovery 11 zapamiętuje zmiany wprowadzone na stronach czynności. Jeśli na przykład rozpocznesz definiowanie planu tworzenia kopii zapasowych, a następnie nie ukończysz go i z dowolnego powodu przełączysz się na inny widok, możesz następnie kliknąć przycisk nawigacji **Wstecz** w menu. Ewentualnie, po wykonaniu kilku kroków, możesz kliknąć strzałkę **w dół** i wybrać z listy stronę, na której rozpoczęło się tworzenie planu. Dzięki temu można wykonać pozostałe kroki i ukończyć tworzenie planu tworzenia kopii zapasowych.



Przyciski nawigacyjne

2.1.3 Opcje konsoli

Opcje konsoli określają sposób przedstawiania informacji w graficznym interfejsie użytkownika programu Acronis Backup & Recovery 11.

Aby uzyskać dostęp do opcji konsoli, należy wybrać z górnego menu kolejno: **Opcje > Konsola**.

Opcje wyświetlania alertów

Opcja ta określa, które alerty będą wyświetlane, a które ukrywane w widoku **Alerty**.

Ustawienie wstępne: **Wszystkie alerty**.

Aby wyświetlić (ukryć) alerty, zaznacz (anuluj zaznaczenie) pola wyboru obok odpowiednich typów alertów.

Pamięć podręczna poświadczeń

Opcja określa, czy poświadczenia wprowadzone podczas korzystania z konsoli zarządzania powinny być przechowywane.

Ustawienie wstępne: **Wyłączone**.

Jeśli opcja jest wyłączona, poświadczenia dostępu do poszczególnych lokalizacji wprowadzane podczas sesji konsoli są przechowywane tylko do momentu zamknięcia konsoli.

Jeśli opcja jest włączona, poświadczenia są przechowywane do wykorzystania podczas kolejnych sesji. W systemie Windows poświadczenia są przechowywane w Menedżerze poświadczeń systemu Windows. W systemie Linux poświadczenia są przechowywane w specjalnym, zaszyfrowanym pliku.

Czcionki

Opcja określa czcionki używane w graficznym interfejsie użytkownika programu Acronis Backup & Recovery 11. Ustawienie **Czcionka menu** dotyczy menu rozwijanych i kontekstowych. Ustawienie **Czcionka aplikacji** dotyczy wszystkich pozostałych elementów interfejsu użytkownika.

Ustawienie wstępne: **Domyślna systemowa** czcionka zarówno w menu, jak i elementach interfejsu aplikacji.

Aby dokonać wyboru, wybierz czcionkę z odpowiedniego pola kombi i ustaw jej właściwości. Wygląd czcionki można sprawdzić, klikając przycisk **Przeglądaj** po prawej stronie.

Komunikaty wyskakujące

Te opcje są dostępne, gdy konsola jest podłączona do komputera zarządzanego lub serwera zarządzania.

Okno dialogowe „Działania wymagające interwencji”

Opcja ta określa, czy w przypadku wystąpienia jednego lub kilku zadań wymagających działania użytkownika ma być wyświetlany komunikat wyskakujący. W oknie tego komunikatu można podjąć jedną decyzję dotyczącą wszystkich działań, na przykład potwierdzić ponowne uruchomienie systemu lub spowodować podjęcie ponownej próby po zwolnieniu miejsca na dysku. Dopóki co najmniej jedno działanie wymaga interwencji użytkownika, można w dowolnym momencie otworzyć to okno na ekranie powitalnym komputera zarządzanego. Można również sprawdzić stany wykonywania zadań w widoku **Plany i zadania tworzenia kopii zapasowych** i określić decyzje dotyczące poszczególnych zadań w panelu Informacje.

Ustawienie wstępne: **Włączone**.

Aby dokonać wyboru, zaznacz lub wyczyść pole wyboru okna dialogowego „Działania wymagające interwencji”.

Okno dialogowe „Potwierdzenie opinii”

Ta opcja określa, czy wyświetlać okno wyskakujące z informacją o stanie systemu po wystąpieniu błędu. Informacje te można wysłać do działu pomocy technicznej firmy Acronis.

Ustawienie wstępne: **Włączone**.

Aby dokonać wyboru, zaznacz lub wyczyść pole wyboru okna dialogowego „Potwierdzenie opinii”.

Powiadom, jeśli nośnik startowy nie został utworzony

Opcja ta określa, czy w przypadku uruchomienia na komputerze konsoli zarządzania i nieutworzenia na nim nośnika startowego ma być wyświetlane okno wyskakujące.

Ustawienie wstępne: **Włączone**.

Aby dokonać wyboru, zaznacz lub wyczyść pole wyboru **Powiadom, jeśli nośnik startowy nie został utworzony**.

Powiadamiaj, gdy konsola zarządzania jest podłączona do innej wersji komponentu

Ta opcja określa, czy wyświetlać okno wyskakujące, gdy konsola jest połączona z agentem/serwerem zarządzania i ich wersje się różnią.

Ustawienie wstępne: **Włączone**.

Aby dokonać wyboru, zaznacz lub wyczyść pole wyboru **Powiadamiaj, gdy konsola zarządzania jest podłączona do innej wersji komponentu**.

Informacje na temat wyników wykonania zadania

Ta opcja jest uwzględniana tylko wtedy, gdy konsola jest połączona z komputerem zarządzanym.

Określa ona, czy wyświetlać komunikaty wyskakujące, które informują o wyniku wykonywania zadania: zakończone pomyślnie, zakończone niepowodzeniem lub zakończone pomyślnie z ostrzeżeniami. Gdy wyświetlanie komunikatów wyskakujących jest wyłączone, stan i wynik wykonywania zadań można sprawdzić w widoku **Plany i zadania tworzenia kopii zapasowych**.

Ustawienie wstępne: **Włączone** dla wszystkich wyników.

Aby określić ustawienie dla poszczególnych wyników, (zakończone pomyślnie, zakończone niepomyślnie lub pomyślnie z ostrzeżeniami), należy zaznaczyć lub anulować zaznaczenie pola wyboru obok odpowiedniej opcji.

Strona początkowa

Ta opcja określa, czy po podłączeniu konsoli do serwera zarządzania ma być wyświetlany ekran **Witamy**, czy widok **Pulpit nawigacyjny**.

Ustawienie wstępne: ekran **Witamy**.

Aby dokonać wyboru, zaznacz lub wyczyść pole wyboru **Pokaż widok „Pulpit nawigacyjny”**.

Opcję tę można także ustawić na ekranie **Witamy**. Jeśli na ekranie **Witamy** zaznaczysz pole wyboru **Po uruchomieniu wyświetlaj pulpit nawigacyjny zamiast bieżącego widoku**, powyższe ustawienie zostanie odpowiednio zaktualizowane.

3 Opis programu Acronis Backup & Recovery 11

W tej sekcji podjęto próbę przystępnego opisanie programu, aby umożliwić czytelnikom korzystanie z niego w różnych okolicznościach bez konieczności odwoływania się do szczegółowych instrukcji.

3.1 Właściciele i poświadczenia

W tej sekcji wyjaśniono pojęcie właściciela oraz znaczenie poświadczeń planu (lub zadania) tworzenia kopii zapasowych.

Właściciel planu (zadania)

Właścicielem lokalnego planu tworzenia kopii zapasowych jest użytkownik, który utworzył lub jako ostatni zmodyfikował ten plan.

Właścicielem scentralizowanego planu tworzenia kopii zapasowych jest administrator serwera zarządzania, który utworzył lub jako ostatni zmodyfikował ten plan.

Właścicielem zadań należących do planu tworzenia kopii zapasowych (lokalnego lub scentralizowanego) jest właściciel tego planu.

Właścicielem zadań nienależących do planu tworzenia kopii zapasowych, takich jak zadanie odzyskiwania, jest użytkownik, który utworzył lub jako ostatni zmodyfikował zadanie.

Zarządzanie planem (zadaniem), którego właścicielem jest inny użytkownik

Użytkownik z uprawnieniami administratora na komputerze może modyfikować zadania i lokalne plany tworzenia kopii zapasowych, których właścicielem jest dowolny użytkownik zarejestrowany w systemie operacyjnym.

Otwarcie do edycji planu lub zadania, którego właścicielem jest inny użytkownik, powoduje wyczyszczenie wszystkich haseł ustawionych w zadaniu. Zapobiega to stosowaniu sztuczki polegającej na zmodyfikowaniu ustawień i pozostawieniu haseł. Przy każdej próbie edycji planu (zadania) zmodyfikowanego ostatnio przez innego użytkownika program wyświetla ostrzeżenie. Po wyświetleniu ostrzeżenia dostępne są dwie możliwości:

- Kliknięcie przycisku **Anuluj** i utworzenie własnego planu lub zadania. Oryginalne zadanie pozostanie niezmienione.
- Kontynuowanie edycji. Należy wówczas wprowadzić wszystkie poświadczenia wymagane do wykonania planu lub zadania.

Właściciel archiwum

Właścicielem archiwum jest użytkownik, który zapisał je w miejscu docelowym. Dokładniej jest to użytkownik, którego konto zostało określone podczas definiowania planu tworzenia kopii zapasowych w kroku **Miejsce docelowe kopii zapasowej**. Domyślnie używane są poświadczenia planu.

Poświadczenia planu i poświadczenia zadania

Każde zadanie jest uruchamiane na komputerze w imieniu określonego użytkownika. Podczas tworzenia planu lub zadania dostępna jest opcja bezpośredniego wskazania konta, na którym będzie

uruchamiany plan lub zadanie. Wybór zależy od tego, czy plan lub zadanie mają być uruchamiane ręcznie czy zgodnie z harmonogramem.

Uruchamianie ręczne

Krok **Poświadczenia planu (zadania)** można pominąć. Zadanie za każdym razem będzie uruchamiane z poświadczeniami, z którymi aktualnie jest zalogowany użytkownik. Zadanie może również uruchomić dowolna osoba mająca uprawnienia administratora na danym komputerze. Zostanie ono uruchomione z poświadczeniami tej osoby.

Jeśli poświadczenia zadania zostaną określone bezpośrednio, zadanie będzie zawsze wykonywane z tymi samymi poświadczeniami, niezależnie od tego, który użytkownik faktycznie je uruchamia. Aby określić poświadczenia, na stronie tworzenia planu (zadania):

1. W sekcji **Parametry planu** (lub **Parametry zadania**) kliknij **Pokaż poświadczenia, komentarze, etykietę planu** (lub **Pokaż poświadczenia zadania**).
2. Kliknij **Poświadczenia planu (zadania)**.
3. Wprowadź poświadczenia, z którymi będzie uruchamiany plan (zadanie).

Uruchamianie zaplanowane lub opóźnione

Poświadczenia planu (zadania) są obowiązkowe. Pominięcie kroku dotyczącego poświadczeń spowoduje, że po zakończeniu tworzenia planu (zadania) zostanie wyświetlony monit o podanie poświadczeń.

Dlaczego program zmusza do określenia poświadczeń?

Zaplanowane lub opóźnione zadanie musi się rozpocząć niezależnie od tego, czy jest zalogowany jakikolwiek użytkownik (na przykład podczas wyświetlania ekranu powitalnego systemu Windows), czy też zalogowany jest użytkownik inny niż właściciel zadania. Wystarczy, że o zaplanowanej godzinie rozpoczęcia zadania komputer będzie włączony (czyli nie będzie w trybie wstrzymania ani hibernacji). Dlatego harmonogram Acronis wymaga bezpośredniego określenia poświadczeń, aby mógł uruchomić zadanie.

3.2 Uprawnienia użytkownika na zarządzanym komputerze

Windows

Podczas zarządzania komputerem z systemem Windows zakres uprawnień użytkownika związanych z zarządzaniem zależy od jego uprawnień na komputerze.

Zwykli użytkownicy

Zwykły użytkownik, na przykład należący do grupy Użytkownicy, ma następujące uprawnienia do zarządzania:

- Tworzenie kopii zapasowych na poziomie plików i odzyskiwanie plików, do których użytkownik ma prawa dostępu — ale bez używania migawek na poziomie plików.
- Definiowanie planów i zadań tworzenia kopii zapasowych oraz zarządzanie nimi.
- Wyświetlanie — ale bez możliwości zarządzania — planów i zadań tworzenia kopii zapasowych. zdefiniowanych przez innych użytkowników.
- Wyświetlanie lokalnego dziennika zdarzeń.

Administratorzy

Użytkownik z uprawnieniami administratora, na przykład należący do grupy Administratorzy lub Operatorzy kopii zapasowych, ma następujące dodatkowe uprawnienia do zarządzania:

- Tworzenie kopii zapasowych i odzyskiwanie całego komputera lub dowolnych znajdujących się na nim danych, w tym również z użyciem migawek dysku.

Użytkownicy należący do grupy Administratorzy mają również następujące uprawnienia:

- Wyświetlanie planów i zadań tworzenia kopii zapasowych należących do dowolnego użytkownika danego komputera oraz zarządzanie nimi.

Linux

Podczas zarządzania komputerem z systemem Linux użytkownik uzyskuje uprawnienia użytkownika root:

- Tworzenie kopii zapasowych i odzyskiwanie danych lub całego komputera przy zachowaniu pełnej kontroli nad wszystkimi działaniami agenta programu Acronis Backup & Recovery 11 oraz plikami dzienników na komputerze.
- Zarządzanie lokalnymi planami i zadaniami tworzenia kopii zapasowych należącymi do dowolnego użytkownika zarejestrowanego w systemie operacyjnym.

Aby uniknąć rutynowego logowania się w systemie jako użytkownik root, można zalogować się jako zwykły użytkownik, a następnie w razie potrzeby przełączyć użytkownika.

3.3 Pełne, przyrostowe i różnicowe kopie zapasowe

Program Acronis Backup & Recovery 11 umożliwia korzystanie z popularnych schematów tworzenia kopii zapasowych, takich jak Dziadek-ojciec-syn i Wieża Hanoi, a także tworzenie niestandardowych schematów tworzenia kopii zapasowych. Wszystkie schematy tworzenia kopii zapasowych są oparte na metodach tworzenia pełnych, przyrostowych i różnicowych kopii zapasowych. Termin „schemat” tak naprawdę oznacza algorytm stosowania tych metod oraz algorytm czyszczenia archiwum.

Porównywanie ze sobą metod tworzenia kopii zapasowych nie ma większego sensu, ponieważ w schemacie tworzenia kopii zapasowych działają one zespołowo. Każda metoda powinna pełnić określoną rolę, w zależności od jej zalet. Profesjonalny schemat tworzenia kopii zapasowych wykorzystuje zalety wszystkich metod tworzenia kopii zapasowych, ograniczając wpływ wszystkich wad tych metod. Na przykład cotygodniowa różnicowa kopia zapasowa zawiera czyszczenie archiwum, ponieważ może zostać łatwo usunięta wraz z cotygodniowym zestawem zależnych od niej codziennych przyrostowych kopii zapasowych.

Proces tworzenia kopii zapasowej metodą pełną, przyrostową lub różnicową powoduje utworzenie kopii zapasowej (s. 380) odpowiedniego typu.

Pełna kopia zapasowa

Pełna kopia zapasowa przechowuje wszystkie dane wybrane do utworzenia kopii zapasowej. Pełna kopia zapasowa stanowi podstawę każdego archiwum i tworzy podwaliny pod przyrostowe oraz różnicowe kopie zapasowe. Archiwum może zawierać wiele pełnych kopii zapasowych lub składać się wyłącznie z pełnych kopii zapasowych. Pełna kopia zapasowa jest samowystarczalna — odzyskanie danych z pełnej kopii zapasowej nie wymaga dostępu do żadnej innej kopii zapasowej.

Powszechnie akceptowany jest fakt, że wykonanie pełnej kopii zapasowej trwa najdłużej, ale jej przywrócenie jest najszybsze. Dzięki technologiom firmy Acronis odzyskiwanie z przyrostowej kopii zapasowej nie musi być wolniejsze niż odzyskiwanie z kopii pełnej.

Pełna kopia zapasowa jest najbardziej przydatna, gdy:

- trzeba przywrócić system do stanu początkowego;
- stan początkowy nie zmienia się często, dzięki czemu nie trzeba regularnie tworzyć kopii zapasowych.

Przykład: Kawiarenka internetowa, szkoła lub laboratorium uniwersyteckie, gdzie administrator często cofa zmiany wprowadzone przez uczniów/studentów lub klientów, natomiast rzadko aktualizuje referencyjną kopię zapasową (tak naprawdę tylko po zainstalowaniu aktualizacji oprogramowania). W takim przypadku czas tworzenia kopii zapasowej nie ma większego znaczenia, a czas odzyskiwania systemów z pełnej kopii zapasowej będzie minimalny. W celu zapewnienia większej niezawodności administrator może mieć kilka egzemplarzy kopii zapasowej.

Przyrostowa kopia zapasowa

Przyrostowa kopia zapasowa przechowuje zmiany danych w porównaniu do **ostatniej kopii zapasowej**. Odzyskanie danych z przyrostowej kopii zapasowej wymaga dostępu do innych kopii zapasowych z tego samego archiwum.

Przyrostowa kopia zapasowa jest najbardziej przydatna, gdy:

- trzeba zachować możliwość przywracania dowolnego z wielu zapisanych stanów;
- zmiany danych są raczej niewielkie w porównaniu z całkowitym rozmiarem danych.

Powszechnie akceptowany jest fakt, że przyrostowe kopie zapasowe są mniej niezawodne niż kopie pełne, ponieważ uszkodzenie jednej kopii zapasowej w „łańcuchu” powoduje, że nie można więcej używać następnych kopii. Jednak gdy potrzebnych jest wiele wcześniejszych wersji danych, przechowywanie wielu pełnych kopii zapasowych nie jest dobrym rozwiązaniem, ponieważ niezawodność zbyt dużego archiwum jest jeszcze bardziej wątpliwa.

Przykład: Tworzenie kopii zapasowej dziennika transakcji bazy danych.

Różnicowa kopia zapasowa

Różnicowa kopia zapasowa przechowuje zmiany danych w porównaniu do **najnowszej pełnej kopii zapasowej**. Odzyskanie danych z różnicowej kopii zapasowej wymaga dostępu do odpowiedniej pełnej kopii zapasowej. Różnicowa kopia zapasowa jest najbardziej przydatna, gdy:

- użytkownik jest zainteresowany zapisywaniem wyłącznie najnowszego stanu danych;
- zmiany danych są raczej niewielkie w porównaniu z całkowitym rozmiarem danych.

Typowy wniosek jest następujący: „tworzenie różnicowych kopii zapasowych trwa dłużej, a ich przywracanie krócej, natomiast tworzenie kopii przyrostowych jest szybsze, a ich przywracanie trwa dłużej”. Tak naprawdę nie ma fizycznej różnicy między przyrostową kopią zapasową dołączoną do pełnej kopii zapasowej a różnicową kopią zapasową dołączoną do tej samej pełnej kopii zapasowej w tym samym punkcie w czasie. Wspomniana powyżej różnica zakłada utworzenie różnicowej kopii zapasowej po (lub zamiast) utworzeniu wielu przyrostowych kopii zapasowych.

Przyrostowa lub różnicowa kopia zapasowa utworzona po defragmentacji dysku może być znacznie większa niż zwykle, ponieważ defragmentacja powoduje zmianę lokalizacji plików na dysku, a kopia zapasowa odzwierciedla te zmiany. Po defragmentacji dysku zaleca się ponowne utworzenie pełnej kopii zapasowej.

W poniższej tabeli podsumowano zalety i wady poszczególnych typów kopii zapasowych w oparciu o popularną wiedzę na ich temat. W rzeczywistości te parametry zależą od wielu czynników, między innymi ilości, szybkości i wzorca zmian danych, natury danych, specyfikacji fizycznych urządzeń,

ustawionych opcji tworzenia kopii zapasowych/odzyskiwania. Najlepszą pomocą przy wybieraniu optymalnego schematu tworzenia kopii zapasowych jest doświadczenie.

Parametr	Pełna kopia zapasowa	Różnicowa kopia zapasowa	Przyrostowa kopia zapasowa
Miejsce do przechowywania	Maksymalne	Średnie	Minimalne
Czas tworzenia	Maksymalny	Średni	Minimalny
Czas odzyskiwania	Minimalny	Średni	Maksymalny

3.4 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 takiej kopii zapasowej można odzyskać całe dyski lub woluminy, jak również poszczególne pliki lub foldery.

Jeśli jest włączona opcja „sektor po sektorze” (tryb „surowych” danych), w kopii zapasowej dysku zostają zapisane wszystkie sektory dysku.

Gdy opcja kopiowania „sektor po sektorze” jest wyłączona, kopia zapasowa dysku lub woluminu z obsługiwanym systemem plików zawiera wyłącznie sektory z danymi. Zmniejsza to rozmiar wynikowej kopii zapasowej oraz przyspiesza operacje jej tworzenia i odzyskiwania danych.

Windows

Przy tworzeniu kopii zapasowej nie jest uwzględniany plik wymiany (pagefile.sys) ani 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.

Kopia zapasowa woluminu zawiera wszystkie pozostałe 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 rozruchowym (MBR). Przy tworzeniu kopii zapasowej nie jest uwzględniany kod startowy woluminów GPT.

Kopia zapasowa dysku zawiera wszystkie woluminy wybranego dysku (w tym woluminy ukryte, takie jak partycje konserwacyjne producenta) oraz ścieżkę zerową głównego rekordu rozruchowego.

Linux

Kopia zapasowa woluminu zawiera wszystkie pliki i foldery 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.

3.5 Informacje na temat woluminów dynamicznych i logicznych

3.5.1 Tworzenie kopii zapasowych woluminów dynamicznych i ich odzyskiwanie (system Windows)

W tej sekcji omówiono w zarysie, jak tworzyć kopie zapasowe woluminów dynamicznych (s. 387) i odzyskiwać je przy użyciu programu Acronis Backup & Recovery 11.

Wolumin dynamiczny to wolumin znajdujący się na dyskach dynamicznych (s. 377), a dokładniej w grupie dysków (s. 378). Program Acronis Backup & Recovery 11 obsługuje następujące typy woluminów dynamicznych/poziomy macierzy RAID:

- prosty/łączony,
- rozłożony (RAID 0),
- lustrzany (RAID 1),
- lustrzany-rozłożony (RAID 0+1),
- RAID -5.

Tworzenie kopii zapasowych woluminów dynamicznych

Kopie zapasowe woluminów dynamicznych są tworzone tak samo jak kopie woluminów standardowych. Podczas definiowania planu tworzenia kopii zapasowych za pośrednictwem graficznego interfejsu użytkownika wszystkie typy woluminów są dostępne do wyboru jako **Elementy uwzględniane w kopii zapasowej**. W przypadku korzystania z wiersza polecenia woluminy dynamiczne należy określić za pomocą prefiksu DYN.

Przykłady wiersza polecenia

```
acrocmbd backup disk --volume=DYN1,DYN2 --loc=\\srv1\backups --  
credentials=netuser1,pass1 --arc=dyn1_2_arc
```

Spowoduje to utworzenie kopii zapasowych woluminów DYN1 i DYN2 w udostępnionym folderze sieciowym.

```
acrocmbd backup disk --volume=DYN --loc=\\srv1\backups --  
credentials=netuser1,pass1 --arc=alldyn_arc
```

Spowoduje to utworzenie kopii zapasowych wszystkich woluminów dynamicznych komputera lokalnego w udostępnionym folderze sieciowym.

Odzyskiwanie woluminów dynamicznych

Wolumin dynamiczny można odzyskać:

- na istniejącym woluminie dowolnego typu;
- do nieprzydzielonego miejsca w grupie dysków;
- do nieprzydzielonego miejsca na dysku standardowym;
- na dysku, który nie został zainicjowany.

Odzyskiwanie na istniejącym woluminie

Gdy wolumin dynamiczny jest odzyskiwany na istniejącym woluminie (standardowym lub dynamicznym), dane na woluminie docelowym są zastępowane zawartością kopii zapasowej. Typ woluminu docelowego (standardowy, prosty/łączony, rozłożony, lustrzany, RAID 0+1, RAID -5) nie ulega zmianie. Rozmiar woluminu docelowego musi być wystarczający, aby pomieścić zawartość kopii zapasowej.

Odzyskiwanie do nieprzydzielonego miejsca w grupie dysków

W przypadku odzyskiwania woluminu dynamicznego do nieprzydzielonego miejsca w grupie dysków zachowywany jest oryginalny typ i rozmiar woluminu. Jeśli konfiguracja grupy dysków nie pozwala na utworzenie woluminu oryginalnego typu, zostanie on odzyskany jako wolumin prosty lub łączony. Jeśli ilość nieprzydzielonego miejsca nie będzie wystarczająca, rozmiar woluminu zostanie zmieniony przez zmniejszenie ilości wolnego miejsca.

Przykłady sytuacji, w których konfiguracja grupy dysków nie pozwala na utworzenie woluminu oryginalnego typu

Przykład 1. Grupa obejmuje mniej dysków, niż wymaga tego wolumin dynamiczny. Załóżmy, że zamierzasz odzyskać do grupy składającej się z dwóch dysków wolumin RAID-5 o pojemności 80 GB, który znajdował się wcześniej na trzech dyskach. Całkowity rozmiar nieprzydzielonego miejsca wynosi 100 GB: 40 GB na pierwszym dysku i 60 GB na drugim. Wolumin RAID-5 zostanie odzyskany jako wolumin łączony rozmieszczony na dwóch dyskach.

Przykład 2. Rozkład nieprzydzielonego miejsca nie umożliwia odzyskania woluminów dynamicznych określonych typów. Załóżmy, że wolumin rozłożony o rozmiarze 30 GB ma zostać odzyskany do grupy dysków obejmującej dwa dyski. Całkowity rozmiar nieprzydzielonego miejsca wynosi 50 GB: 10 GB na pierwszym dysku i 40 GB na drugim. Wolumin rozłożony zostanie odzyskany jako wolumin prosty na drugim dysku.

Odzyskiwanie na dysku, który nie został zainicjowany

W takim przypadku dysk docelowy zostanie automatycznie zainicjowany w stylu partycjonowania MBR. Woluminy dynamiczne zostaną odzyskane jako woluminy standardowe. Jeśli nie zmieszczą się na nieprzydzielonym miejscu, ich rozmiar zostanie proporcjonalnie zmieniony (przez zmniejszenie ilości wolnego miejsca).

W poniższej tabeli znajdują się typy woluminów wynikowych zależne od źródła kopii zapasowej oraz woluminu docelowego odzyskiwania.

	Kopia zapasowa (źródło):	
Miejsce odzyskiwania:	Wolumin dynamiczny	Wolumin standardowy
Wolumin dynamiczny	Wolumin dynamiczny Takiego samego typu jak miejsce docelowe	Wolumin dynamiczny Takiego samego typu jak miejsce docelowe
Nieprzydzielone miejsce (grupa dysków)	Wolumin dynamiczny Takiego samego typu jak źródło	Wolumin dynamiczny Prosty
Wolumin standardowy lub nieprzydzielone miejsce na dysku standardowym	Wolumin standardowy	Wolumin standardowy

Przenoszenie i zmiana rozmiaru woluminów podczas odzyskiwania

Podczas odzyskiwania można ręcznie zmienić rozmiar wynikowego woluminu standardowego lub jego lokalizację na dysku. Nie można ręcznie zmienić lokalizacji ani rozmiaru wynikowego woluminu dynamicznego.

Przygotowywanie grup dysków i woluminów

Przed odzyskiwaniem woluminów dynamicznych od podstaw należy na sprzęcie docelowym utworzyć grupę dysków.

Może być także konieczne utworzenie lub zwiększenie nieprzydzielonego miejsca w istniejącej grupie dysków. W tym celu można usunąć woluminy lub przekonwertować dyski standardowe na dynamiczne.

Można zmienić typ woluminu docelowego (standardowy, prosty/łączony, rozłożony, lustrzany, RAID 0+1, RAID 5). W tym celu należy usunąć wolumin docelowy i w uzyskanym nieprzydzielonym miejscu utworzyć nowy wolumin.

Program Acronis Backup & Recovery 11 zawiera wygodne narzędzie do zarządzania dyskami, które umożliwia wykonanie powyższych operacji zarówno w systemie operacyjnym, jak i na nowym

sprzęcie bez systemu operacyjnego. Więcej informacji na temat narzędzia Acronis Disk Director Lite można znaleźć w sekcji Zarządzanie dyskami (s. 264).

3.5.2 Tworzenie kopii zapasowych i odzyskiwanie woluminów logicznych i urządzeń MD (system Linux)

W tej sekcji został przedstawiony sposób tworzenia kopii zapasowych oraz odzyskiwania woluminów zarządzanych przez menedżer dysków logicznych systemu Linux (ang. Logical Volume Manager, LVM) nazywanych woluminami logicznymi, oraz urządzeń z wieloma dyskami (ang. multiple-disk, MD) nazywanych programowymi urządzeniami RAID systemu Linux.

Aby dowiedzieć się więcej na temat menedżera dysków logicznych, odwiedź stronę <http://tldp.org/HOWTO/LVM-HOWTO/> lub http://www.centos.org/docs/5/html/5.1/Deployment_Guide/ch-lvm.html.

Tworzenie kopii zapasowych woluminów logicznych

Komponent Acronis Backup & Recovery 11 Agent for Linux umożliwia dostęp do woluminów logicznych, tworzenie ich kopii zapasowych oraz ich odzyskiwanie w systemie Linux z jądrem 2.6.x lub przy użyciu nośnika startowego opartego na systemie Linux.

Kopia zapasowa

W graficznym interfejsie użytkownika programu Acronis Backup & Recovery 11 woluminy logiczne są wyświetlane w sekcji **Woluminy dynamiczne** na końcu listy woluminów dostępnych do tworzenia kopii zapasowych. Jeśli wybierzesz tworzenie kopii zapasowych woluminów logicznych, struktura woluminów logicznych zostanie zapisana w kopii zapasowej wraz z ich zawartością. Umożliwia to automatyczne odtworzenie struktury w przypadku odzyskiwania tych woluminów za pomocą nośnika startowego opartego na systemie Linux.

Aby utworzyć kopię zapasową wszystkich dostępnych dysków, należy określić wszystkie woluminy logiczne oraz woluminy standardowe, które nie należą do tych woluminów logicznych. Jest to opcja domyślna po otwarciu strony **Utwórz plan tworzenia kopii zapasowych**.

Na liście wyświetlane są woluminy standardowe zawarte w woluminach logicznych, oznaczone jako **Brak** w kolumnie **System plików**. Jeśli wybierzesz takie woluminy, program będzie tworzył ich kopie zapasowe metodą „sektor po sektorze”. Zwykle nie jest to wymagane.

Odzyskiwanie

W przypadku odzyskiwania woluminów logicznych dostępne są dwie opcje:

- **Odzyskiwanie tylko zawartości woluminów.** Typ i inne właściwości woluminu docelowego nie ulegają zmianie.

Ta opcja jest dostępna zarówno po uruchomieniu programu w systemie operacyjnym, jak i przy użyciu nośnika startowego.

Ta opcja jest przydatna w następujących przypadkach:

- Gdy nastąpiła utrata części danych z woluminu, ale nie wymieniono dysków twardych.
- Podczas odzyskiwania woluminu logicznego na dysk lub wolumin standardowy. W takim przypadku możesz zmienić rozmiar woluminu wynikowego.

Nie jest możliwe uruchomienie systemu odzyskanego z woluminu logicznego na dysk standardowy, ponieważ jądro systemu próbuje zamontować główny system plików na woluminie logicznym. Aby

uruchomić system, należy zmienić konfigurację programu ładującego i plik `/etc/fstab`, tak aby nie było używane narzędzie LVM, a następnie aktywować ponownie program ładujący (s. 163).

- Podczas odzyskiwania woluminu standardowego lub logicznego na utworzony wcześniej wolumin logiczny. Taka sytuacja może wystąpić, gdy utworzysz strukturę woluminów logicznych ręcznie (s. 42) przy użyciu narzędzia **lvm**.
- **Odzyskiwanie struktury oraz zawartości woluminów logicznych.**

Taka sytuacja może wystąpić podczas odzyskiwania na komputerze bez zainstalowanego systemu operacyjnego, lub na komputerze o innej strukturze woluminów. Strukturę woluminów logicznych można automatycznie utworzyć podczas odzyskiwania (s. 41).

Ta opcja jest dostępna tylko podczas pracy z nośnikiem startowym.

Szczegółowe instrukcje dotyczące odzyskiwania woluminów logicznych zawiera sekcja Odzyskiwanie urządzeń MD i woluminów logicznych (s. 41).

Tworzenie kopii zapasowych urządzeń MD

Urządzenia MD, nazywane również programowymi urządzeniami RAID systemu Linux, łączą kilka woluminów i stanowią urządzenia blokowe (`/dev/md0`, `/dev/md1`, ..., `/dev/md31`). Informacje na temat urządzeń MD są przechowywane w katalogu `/etc/raidtab` lub w wydzielonych obszarach tych woluminów.

Kopie zapasowe aktywnych (zamontowanych) urządzeń MD można tworzyć w taki sam sposób jak kopie woluminów logicznych. Urządzenia MD znajdują się na końcu listy woluminów dostępnych do utworzenia kopii zapasowej. W przypadku tworzenia kopii zapasowej urządzeń MD ich struktura zostanie zapisana w kopii wraz z ich zawartością.

Tworzenie kopii zapasowych woluminów znajdujących się na zamontowanych urządzeniach MD nie ma sensu, ponieważ ich odzyskanie będzie niemożliwe.

Podczas odzyskiwania urządzeń MD przy użyciu nośnika startowego możesz automatycznie odtworzyć ich strukturę. Aby uzyskać szczegółowe informacje na temat odzyskiwania urządzeń MD przy użyciu nośnika startowego, zobacz Odzyskiwanie urządzeń MD i woluminów logicznych (s. 41).

Aby uzyskać informacje na temat składania urządzeń MD podczas odzyskiwania w systemie Linux, zobacz Składanie urządzeń MD do odzyskiwania (Linux) (s. 40).

Tworzenie kopii zapasowych sprzętowych macierzy RAID (Linux)

Sprzętowe macierze RAID w systemie Linux łączą kilka dysków fizycznych, tworząc pojedynczy dysk, który można podzielić na partycje. Specjalny plik związany ze sprzętową macierzą RAID zazwyczaj znajduje się w katalogu `/dev/ataraid`. Kopie zapasowe sprzętowych macierzy RAID można tworzyć w taki sam sposób jak kopie zapasowe zwykłych dysków twardych.

Dyski fizyczne wchodzące w skład sprzętowych macierzy RAID mogą być wyświetlane obok innych dysków tak, jakby miały nieprawidłową tabelę partycji lub w ogóle nie miały tabeli partycji. Tworzenie kopii zapasowych takich dysków nie ma sensu, ponieważ ich odzyskanie będzie niemożliwe.

Składanie urządzeń MD do odzyskiwania (Linux)

W systemie Linux przed odzyskaniem danych z kopii zapasowej dysku na istniejące urządzenie MD (zwane również programowym urządzeniem RAID systemu Linux) należy się upewnić, że **urządzenie zostało złożone**.

Jeśli tak nie jest, należy je złożyć przy użyciu narzędzia **mdadm**. Oto dwa przykłady:

Przykład 1. Następujące polecenie umożliwia złożenie urządzenia `/dev/md0` z woluminów `/dev/sdb1` i `/dev/sdc1`:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb1 /sdc1
```

Przykład 2. Następujące polecenie umożliwia złożenie urządzenia `/dev/md0` z dysków `/dev/sdb` i `/dev/sdc`:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb /dev/sdc
```

Jeśli odzyskanie wymaga ponownego uruchomienia komputera (zwykle wówczas, gdy odzyskiwane woluminy obejmują partycję startową), należy postępować według następujących wskazówek:

- Jeśli wszystkie części urządzenia MD to woluminy (typowy przypadek, tak jak w pierwszym przykładzie), upewnij się, że typ każdego woluminu — nazywany typem partycji lub identyfikatorem systemu — to **Linux raid automount**. Kod szesnastkowy takiego typu partycji to `0xFD`. Gwarantuje to automatyczne złożenie urządzenia po ponownym uruchomieniu komputera. Aby wyświetlić lub zmienić typ partycji, użyj narzędzia do partycjonowania dysków, na przykład **fdisk**.
- W przeciwnym razie (takim, jak w drugim przykładzie) odzyskaj urządzenie z nośnika startowego. Nie jest wówczas wymagane ponowne uruchomienie komputera. Na nośniku startowym może być konieczne ręczne utworzenie urządzenia MD zgodnie z opisem w sekcji Odzyskiwanie urządzeń MD i woluminów logicznych (s. 41).

Odzyskiwanie urządzeń MD i woluminów logicznych

Odzyskiwanie urządzeń MD oraz woluminów utworzonych przez menedżera woluminów logicznych LVM (woluminów logicznych) zakłada odtworzenie odpowiedniej struktury woluminów.

Za pomocą nośnika startowego opartego na systemie Linux można automatycznie utworzyć strukturę woluminów (s. 41) podczas odzyskiwania woluminów z:

- Kopii zapasowej utworzonej przez program Acronis Backup & Recovery 11.
- Kopii zapasowej utworzonej przez program Acronis Backup & Recovery 10, pod warunkiem, że została w niej zapisana informacja o strukturze woluminów (domyślnie jest ona zapisywana).

W pozostałych przypadkach przed rozpoczęciem odzyskiwania należy ręcznie utworzyć strukturę woluminów (s. 42) za pomocą narzędzi **mdadm** i **lv**.

Automatyczne tworzenie struktury woluminów

Za pomocą poniższej procedury utwórz strukturę woluminów na nośniku startowym opartym na systemie Linux.

Uwaga: Jeśli odzyskujesz woluminy z kopii zapasowej utworzonej za pomocą programu Acronis Backup & Recovery 10, ta procedura jest dostępna tylko w przypadku zapisania w kopii zapasowej informacji o strukturze woluminów. (domyślnie jest ona zapisywana).

Przeostroga: Wskutek wykonania poniższej procedury istniejąca w komputerze struktura woluminów zostanie zastąpiona nową, przechowywaną w archiwum. Spowoduje to zniszczenie wszystkich danych znajdujących się obecnie na niektórych lub wszystkich dyskach twardych komputera.

W przypadku zmiany konfiguracji dysków Urządzenie MD lub wolumin logiczny znajduje się na przynajmniej jednym dysku, przy czym każdy dysk może mieć inny rozmiar. Jeśli doszło do zastąpienia dowolnego z dysków w czasie między utworzeniem kopii zapasowej a odzyskiwaniem (lub jeśli

woluminy są odzyskiwane na inny komputer), sprawdź, czy w nowej konfiguracji dysków znajduje się wystarczająca liczba dysków o rozmiarach nie mniejszych niż rozmiary poprzednich dysków.

Aby automatycznie utworzyć strukturę woluminów

1. Uruchom komputer z nośnika startowego opartego na systemie Linux.
2. Kliknij **Acronis Bootable Agent**. Następnie kliknij **Uruchom konsolę zarządzania**.
3. W konsoli zarządzania kliknij **Odzyskaj**.
W sekcji z zawartością archiwum program Acronis Backup & Recovery 11 wyświetli komunikat o wykryciu informacji o strukturze woluminu.
4. W obszarze komunikatu kliknij **Szczegóły**.
5. Zapoznaj się ze strukturą woluminu i, aby ją utworzyć, kliknij **Zastosuj RAID/LVM**.

Ręczne tworzenie struktury woluminów

Poniżej przedstawiono ogólną procedurę odzyskiwania urządzeń MD i woluminów logicznych przy użyciu nośnika startowego opartego na systemie Linux oraz przykład takiego odzyskiwania. W systemie Linux można zastosować podobną procedurę.

Aby ręcznie utworzyć strukturę woluminów

1. Uruchom komputer z nośnika startowego opartego na systemie Linux.
2. Kliknij **Acronis Backup & Recovery 11**. Następnie kliknij **Uruchom konsolę zarządzania**.
3. Na pasku narzędzi kliknij **Czynności**, a następnie kliknij **Uruchom powłokę**. Możesz również nacisnąć klawisze CTRL+ALT+F2.
4. W razie potrzeby sprawdź strukturę woluminów przechowywanych w archiwum, używając narzędzia `acrocmbd`. Narzędzie to może ponadto służyć do zamontowania jednego lub większej liczby tych woluminów tak, jakby były zwykłymi woluminami (zobacz „Montowanie woluminów z kopii zapasowych” w dalszej części tego tematu).
5. Utwórz strukturę woluminów zgodnie ze strukturą zawartą w archiwum, używając narzędzia `mdadm` (w przypadku urządzeń MD), narzędzia `lvm` (w przypadku woluminów logicznych) lub obu tych narzędzi.

Uwaga: Narzędzia Menedżera woluminów logicznych takie jak `pvcreate` i `vgcreate`, zazwyczaj dostępne w systemie Linux, nie są dołączane do środowiska nośnika startowego, dlatego należy użyć narzędzia `lvm` z odpowiednim poleceniem. Na przykład: `lvm pvcreate`, `lvm vgcreate` i `lvm lvcreate`.

6. Jeśli wcześniej kopia zapasowa została zamontowana przy użyciu narzędzia `acrocmbd`, użyj tego narzędzia ponownie, aby odmontować kopię zapasową (zobacz „Montowanie woluminów z kopii zapasowych” w dalszej części tego tematu).
7. Wróć do konsoli zarządzania, naciskając klawisze ALT+F1.
(W tym momencie nie uruchamiaj ponownie komputera. W przeciwnym razie konieczne będzie ponowne utworzenie struktury woluminów).
8. Kliknij **Odzyskaj**, określ ścieżkę do archiwum i wszystkie inne wymagane parametry, a następnie kliknij **OK**.

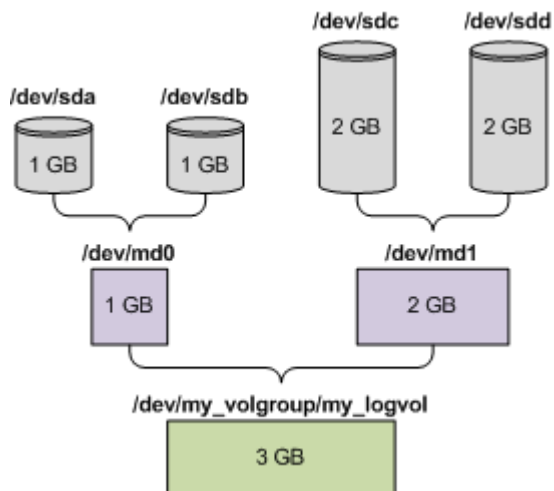
Uwaga: Ta procedura nie ma zastosowania po nawiązaniu zdalnego połączenia z agentem startowym Acronis Backup & Recovery 11 Bootable Agent, ponieważ w takim przypadku powłoka poleceń jest niedostępna.

Przykład

Załóżmy, że została wykonana kopia zapasowa na poziomie dysku komputera o następującej konfiguracji dysków:

- Komputer zawiera dwa dyski twarde SCSI o pojemności 1 GB i dwa takie dyski o pojemności 2 GB, zamontowane odpowiednio w partycjach **/dev/sda**, **/dev/sdb**, **/dev/sdc** i **/dev/sdd**.
- Pierwszą i drugą parę dysków twardych skonfigurowano jako dwa urządzenia MD (oba w konfiguracji RAID-1) i zamontowano odpowiednio w partycjach **/dev/md0** i **/dev/md1**.
- Wolumin logiczny opiera się na tych dwóch urządzeniach MD i jest zamontowany w partycji **/dev/my_volgroup/my_logvol**.

Konfigurację tę przedstawia poniższa ilustracja.



Aby odzyskać dane z tego archiwum, wykonaj poniższe czynności.

Krok 1: Utworzenie struktury woluminów

1. Uruchom komputer z nośnika startowego opartego na systemie Linux.
2. W konsoli zarządzania naciśnij klawisze CTRL+ALT+F2.
3. Uruchom następujące polecenia, aby utworzyć urządzenia MD:

```
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[ab]
mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sd[cd]
```

4. Uruchom następujące polecenia, aby utworzyć grupę woluminu logicznego:

Przestroga: Polecenie *pvccreate* niszczy wszystkie dane na urządzeniach **/dev/md0** i **/dev/md1**.

```
lvm pvccreate /dev/md0 /dev/md1
lvm vgcreate my_volgroup /dev/md0 /dev/md1
lvm vgdisplay
```

Dane wyjściowe polecenia *lvm vgdisplay* będą zawierać wiersze podobne do przedstawionych poniżej:

```
--- Volume group ---
VG Name      my_volgroup
...
VG Access    read/write
VG Status    resizable
...
VG Size      1.99 GB
...
VG UUID      0qoQ4l-Vk7W-yDG3-uF1l-Q2AL-C0z0-vMeACu
```

5. Uruchom poniższe polecenie, aby utworzyć wolumin logiczny. W parametrze **-L** określ rozmiar podany jako **VG Size**:

```
lvm lvcreate -L1.99G --name my_logvol my_volgroup
```

6. Aktywuj grupę woluminu, uruchamiając następujące polecenie:

```
lvm vgchange -a y my_volgroup
```

7. Naciśnij klawisze ALT+F1, aby wrócić do konsoli zarządzania.

Krok 2: Rozpoczęcie odzyskiwania

1. W konsoli zarządzania kliknij **Odzyskaj**.
2. W obszarze **Archiwum** kliknij **Zmień**, a następnie określ nazwę archiwum.
3. W obszarze **Kopia zapasowa** kliknij **Zmień**, a następnie wybierz kopię zapasową, z której chcesz odzyskać dane.
4. W obszarze **Typ danych** wybierz **Woluminy**.
5. W obszarze **Elementy do odzyskiwania** zaznacz pole wyboru obok pozycji **my_volgroup-my_logvol**.
6. W obszarze **Lokalizacja odzyskiwania** kliknij **Zmień**, a następnie wybierz wolumin utworzony w kroku 1. Listę dysków możesz rozwijać przyciskami strzałek.
7. Kliknij **OK**, aby rozpocząć odzyskiwanie.

Aby uzyskać pełną listę poleceń i narzędzi, których można używać w środowisku nośnika startowego, zobacz Lista poleceń i narzędzi dostępnych na nośniku startowym opartym na systemie Linux (s. 259). Aby uzyskać szczegółowe opisy narzędzia **acrocmbd**, zobacz opis wiersza poleceń programu Acronis Backup & Recovery 11.

Montowanie woluminów z kopii zapasowych

Zamontowanie woluminu przechowywanego w kopii zapasowej dysku może być konieczne na przykład w celu wyświetlenia niektórych zawartych w nim plików przed rozpoczęciem odzyskiwania.

Aby zamontować wolumin kopii zapasowej

1. Za pomocą polecenia **acrocmbd list content** wyświetl listę dysków i woluminów przechowywanych w kopii zapasowej. Następujące polecenie umożliwia na przykład wyświetlenie zawartości ostatniej kopii zapasowej zapisanej w archiwum **linux_machine**:

```
acrocmbd list content --loc=\\server\backups --credentials=user,MyPassWd --arc=linux_machine
```

Dane wyjściowe będą zawierać wiersze podobne do przedstawionych poniżej:

type: disk					
Num	Partition	Flags	Size	Type	GUID
-----	-----	-----	-----	-----	-----
--					
Dyn1	my_volgroup-my_lo...		4 GB	Ext 3	
Dyn2	md0		2.007 GB	Ext 2	
Disk 1	sda		16 GB	DT_FIXED	
1-1	sda1	Act,Pri	203.9 MB	Ext 2	
1-2	sda2	Pri	11.72 GB	Reiser	
1-3	sda3	Pri	1.004 GB	Linux swap	
Disk 2	sdb		8 GB	DT_FIXED	
2-1	sdb1	Pri	2.007 GB	Ext 2	
2-2	sdb2	Pri	2.007 GB	None	
Disk 3	sdc		1 GB	DT_FIXED	
Disk 4	sdd		8 GB	DT_FIXED	
4-1	sdd1	Pri	2.007 GB	Ext 2	
4-2	sdd2	Pri	2.007 GB	None	

2. Użyj polecenia **acrocmbd mount**, określając nazwę woluminu w parametrze **--volume**. Na przykład:

```
acrocmd mount --loc=\\server\backups --arc=linux_machine --mount_point=/mnt --volume=DYN1
```

To polecenie spowoduje zamontowanie woluminu logicznego DYN1 w punkcie montowania /mnt.

Aby odmontować wolumin kopii zapasowej

- Użyj polecenia `acrocmd umount`, określając jako parametr punkt montowania woluminu. Na przykład:

```
acrocmd umount --mount_point=/mnt
```

3.6 Kompatybilność z programami szyfrującymi

Program Acronis Backup & Recovery 11 zachowuje pełną funkcjonalność we współpracy z programami do szyfrowania na poziomie pliku.

Programy szyfrujące na poziomie dysku szyfrują 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 Acronis Secure Zone.

Po spełnieniu pewnych warunków program Acronis Backup & Recovery 11 jest kompatybilny z następującymi programami szyfrującymi 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.

Powszechna reguła dotycząca instalacji

Stanowczo zaleca się zainstalowanie programu szyfrującego przed rozpoczęciem instalacji programu Acronis Backup & Recovery 11.

Sposób korzystania z programu Acronis Secure Zone

Strefa Acronis Secure Zone nie może być zaszyfrowana na poziomie dysku. Ze strefy Acronis Secure Zone można korzystać tylko w następujący sposób:

1. Zainstaluj program szyfrujący, a następnie zainstaluj program Acronis Backup & Recovery 11.
2. Utwórz strefę Acronis Secure Zone.
3. Wyklucz strefę Acronis 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. Nie próbuj utworzyć kopii zapasowej za pomocą nośnika startowego ani menedżera Acronis Startup Recovery Manager.

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 odzyskanego systemu nie będzie można uruchomić, odbuduj główny rekord startowy zgodnie z opisem w artykule bazy wiedzy Acronis: „Restoring Windows Boot Loader Manually” (Ręczne odzyskiwanie programu ładującego systemu Windows) i ponownie uruchom komputer.

3.7 Obsługa SNMP

Obiekty SNMP

Program Acronis Backup & Recovery 11 udostępnia następujące obiekty protokołu Simple Network Management Protocol (SNMP) aplikacjom zarządzającym SNMP:

- Typ zdarzenia
Identyfikator obiektu (OID): 1.3.6.1.4.1.24769.100.200.1.0
Składnia: OctetString
Możliwe są następujące wartości: „Informacja”, „Ostrzeżenie”, „Błąd” lub „Nieznane”. Wartość „Nieznane” jest wysyłana tylko w wiadomości próbnej.
- Tekstowy opis zdarzenia
Identyfikator obiektu (OID): 1.3.6.1.4.1.24769.100.200.2.0
Składnia: OctetString
Wartość zawiera opis tekstowy zdarzenia (wygląda identycznie, jak wiadomości publikowane przez program Acronis Backup & Recovery 11 w jego dzienniku).

Przykłady wartości varbind:

1.3.6.1.4.1.24769.100.200.1.0:Informacja

1.3.6.1.4.1.24769.100.200.2.0:I0064000B

Obsługiwane operacje

Program Acronis Backup & Recovery 11 **obsługuje tylko operacje TRAP**. Nie jest możliwe zarządzanie programem Acronis Backup & Recovery 11 przy użyciu żądań GET- i SET-. Oznacza to, że należy używać odbiornika SNMP Trap w celu odbierania wiadomości TRAP.

Informacje na temat bazy informacji zarządzania (MIB)

Plik MIB **acronis-abr.mib** znajduje się w katalogu instalacyjnym programu Acronis Backup & Recovery 11. Domyślnie: %ProgramFiles%\Acronis\BackupAndRecovery w systemie Windows i /usr/lib/Acronis/BackupAndRecovery w systemie Linux.

Ten plik można odczytać przy użyciu przeglądarki plików MIB lub prostego edytora tekstowego, takiego jak Notatnik lub vi.

Informacje na temat wiadomości próbnej

Podczas konfigurowania powiadomień SNMP możesz wysłać wiadomość próbną, aby sprawdzić, czy ustawienia są poprawne.

Parametry wiadomości próbnej są następujące:

- Typ zdarzenia
OID: 1.3.6.1.4.1.24769.100.200.1.0
Wartość: „Nieznane”
- Tekstowy opis zdarzenia
OID: 1.3.6.1.4.1.24769.100.200.2.0
Wartość: „?00000000”

4 Kopia zapasowa

4.1 Utwórz kopię zapasową

Funkcja **Utwórz kopię zapasową** służy do konfigurowania i uruchamiania jednorazowej procedury tworzenia kopii zapasowej w kilku prostych krokach. Proces tworzenia kopii zapasowej rozpocznie się natychmiast po wykonaniu wymaganych kroków i kliknięciu **OK**.

W przypadku długofalowych strategii tworzenia kopii zapasowych obejmujących korzystanie z harmonogramów i warunków, cykliczne usuwanie kopii zapasowych lub przenoszenie ich do innych lokalizacji, należy rozważyć opracowanie planu tworzenia kopii zapasowych.

Konfigurowanie natychmiastowej operacji tworzenia kopii zapasowej przypomina tworzenie planu tworzenia kopii zapasowych (s. 48) z wyjątkiem następujących uwarunkowań:

- Brak jest opcji planowania tworzenia kopii zapasowych i konfigurowania reguł przechowywania.
- Zostanie zastosowane uproszczone nazewnictwo plików kopii zapasowych (s. 70), jeśli jest ono obsługiwane przez lokalizację docelową. W innym razie zostanie zastosowane standardowe nazewnictwo kopii zapasowych.

Uproszczone nazewnictwo plików nie jest obsługiwane przez następujące lokalizacje: skarbce zarządzane, taśmę, strefę Acronis Secure Zone oraz magazyn Acronis Online Backup Storage.

- W ramach operacji tworzenia kopii zapasowej nie jest obsługiwana konwersja kopii zapasowej na poziomie dysku na maszynę wirtualną. Operację taką można przeprowadzić później.

4.2 Tworzenie planu tworzenia kopii zapasowych

Przed utworzeniem pierwszego planu tworzenia kopii zapasowych (s. 382) zapoznaj się z podstawowymi pojęciami stosowanymi w programie Acronis Backup & Recovery 11.

Aby utworzyć plan tworzenia kopii zapasowych, wykonaj poniższe czynności.

Elementy uwzględniane w kopii zapasowej

Elementy uwzględniane w kopii zapasowej (s. 50)

Wybierz typ danych przeznaczonych do kopii zapasowej i określ elementy danych. Typ danych zależy od agentów zainstalowanych na komputerze.

Poświadczenia dostępu, wykluczenia

Aby uzyskać dostęp do tych ustawień, kliknij **Poświadczenia dostępu, wykluczenia**.

Poświadczenia dostępu (s. 52)

Jeśli konto planu nie ma uprawnień dostępu do danych źródłowych, podaj poświadczenia dla danych.

Wykluczenia (s. 52)

Skonfiguruj wykluczenia, określając konkretne typy plików, które nie powinny znaleźć się w kopii zapasowej.

Miejsce docelowe kopii zapasowej

Lokalizacja (s. 65)

Określ ścieżkę do lokalizacji, w której przechowywane będzie archiwum kopii zapasowej, oraz nazwę archiwum. Nazwa archiwum musi być unikatowa w danej lokalizacji. W przeciwnym

razie kopie powstałe w oparciu o nowo utworzony plan tworzenia kopii zapasowych zostaną umieszczone w istniejącym archiwum należącym do innego planu tworzenia kopii zapasowych. Domyślna nazwa to Archiwum(N), gdzie N to kolejny numer archiwum w wybranej lokalizacji.

Nazewnictwo plików kopii zapasowych, poświadczenia dostępu, komentarze dotyczące archiwum

Aby uzyskać dostęp do tych ustawień, kliknij **Pokaż nazewnictwo plików kopii zapasowych, poświadczenia dostępu, komentarze dotyczące archiwum**.

Nazewnictwo plików (s. 70)

[Opcjonalnie] Zaznacz pole wyboru **Plikom kopii zapasowych nadawaj nazwy archiwum, tak jak w programie Acronis True Image Echo, a nie nazwy generowane automatycznie**, jeśli chcesz zastosować w odniesieniu do kopii zapasowych archiwum uproszczone nazewnictwo plików.

Opcja niedostępna w przypadku tworzenia kopii zapasowej w skarbcu zarządzanym, na taśmie, w strefie Acronis Secure Zone lub w magazynie Acronis Online Backup Storage.

Poświadczenia dostępu (s. 54)

[Opcjonalnie] Jeśli konto planu nie ma uprawnień dostępu do lokalizacji, podaj związane z nią poświadczenia.

Komentarze dotyczące archiwum

[Opcjonalnie] Wprowadź komentarze do archiwum.

Sposób tworzenia kopii zapasowej

Schemat tworzenia kopii zapasowych (s. 54)

Określ czas i częstotliwość tworzenia kopii zapasowych danych, zdefiniuj okres przechowywania utworzonych archiwów kopii zapasowych w wybranej lokalizacji oraz ustal harmonogram procedury czyszczenia archiwum (zobacz „Ustawienia replikacji i przechowywania” poniżej). Skorzystaj z dobrze znanych, zoptymalizowanych schematów tworzenia kopii zapasowych, takich jak Dziadek-ojciec-syn i Wieża Hanoi, zdefiniuj schemat niestandardowy lub utwórz kopię zapasową danych jeden raz.

Ustawienia replikacji i przechowywania (s. 90)

Nie są one dostępne w przypadku wyboru uproszczonego nazewnictwa plików kopii zapasowych (s. 70).

Określ, czy kopie zapasowe mają być kopiowane (replikowane) do innej lokalizacji oraz czy mają być przenoszone czy usuwane zgodnie z regułami przechowywania. Dostępne ustawienia zależą od schematu tworzenia kopii zapasowych.

Druga lokalizacja, sprawdzanie poprawności, konwersja na maszynę wirtualną

Aby uzyskać dostęp do tych ustawień, kliknij **Pokaż drugą lokalizację, sprawdzanie poprawności, konwersję na maszynę wirtualną**.

Druga lokalizacja

[Opcjonalnie] Aby skonfigurować replikację kopii zapasowych, zaznacz pole wyboru **Replikuj nowo utworzoną kopię zapasową do innej lokalizacji**. Aby uzyskać więcej informacji na temat replikacji kopii zapasowych, zobacz Konfigurowanie replikacji kopii zapasowych (s. 93).

Czas sprawdzania poprawności (s. 67)

[Opcjonalnie] W zależności od wybranego schematu tworzenia kopii zapasowych zdefiniuj czas i częstotliwość sprawdzania poprawności oraz czy ma być sprawdzana poprawność całego archiwum czy ostatniej kopii zapasowej w tym archiwum.

Konwersja na maszynę wirtualną (s. 99)

[Opcjonalnie] Dotyczy: kopii zapasowej dysku lub woluminu, całych maszyn wirtualnych lub woluminów maszyny wirtualnej.

Skonfiguruj regularną konwersję kopii zapasowej dysku lub woluminu na maszynę wirtualną.

Parametry planu

Nazwa planu

[Opcjonalnie] Wprowadź unikatową nazwę planu tworzenia kopii zapasowych. Dobrze dobrana nazwa umożliwi jego identyfikację pośród innych planów.

Opcje tworzenia kopii zapasowych

[Opcjonalnie] Skonfiguruj parametry operacji tworzenia kopii zapasowej, takie jak polecenia poprzedzające/następujące po tworzeniu kopii, maksymalna przepustowość sieci przydzielona do strumienia kopii zapasowej lub stopień kompresji archiwum. Jeśli w tej sekcji nie wykonasz żadnej czynności, zostaną użyte wartości domyślne (s. 102).

Po zmianie dowolnego z ustawień na wartość różną od domyślnej pojawi się nowy wiersz zawierający nowo skonfigurowaną wartość. Stan ustawienia zmieni się z wartości **Domyślne** na **Przywróć domyślne**. W razie ponownej zmiany ustawienia w wierszu pojawi się nowa wartość, o ile nie będzie to wartość domyślna. W przypadku wartości domyślnej wiersz zniknie. Dlatego w tej sekcji wyświetlane są tylko ustawienia różne od domyślnych.

Aby przywrócić wartości domyślne wszystkich ustawień, kliknij **Przywróć domyślne**.

Poświadczenia, komentarze, etykieta planu

Aby uzyskać dostęp do tych ustawień, kliknij **Pokaż poświadczenia, komentarze, etykietę planu**.

Poświadczenia planu (s. 68)

[Opcjonalnie] Plan tworzenia kopii zapasowych będzie uruchamiany w imieniu użytkownika, który go utworzył. W razie potrzeby poświadczenia planu można zmienić.

Komentarze

[Opcjonalnie] Wpisz opis planu tworzenia kopii zapasowych.

Etykieta (s. 68)

[Opcjonalnie] Wpisz etykietę tekstową dla komputera, którego kopię zapasową chcesz utworzyć. Etykieta umożliwia identyfikację komputera w różnych scenariuszach.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby utworzyć plan tworzenia kopii zapasowych.

Następnie może pojawić się monit o podanie hasła (s. 70).

Utworzony plan będzie dostępny do sprawdzenia i zarządzania w widoku **Plany i zadania tworzenia kopii zapasowych** (s. 282).

4.2.1 Wybieranie danych do uwzględnienia w kopii zapasowej

Aby wybrać dane uwzględniane w kopii zapasowej

1. W sekcji **Dane uwzględniane w kopii zapasowej** wybierz typ danych, które chcesz uwzględnić w kopii zapasowej. Lista dostępnych typów danych zależy od agentów uruchomionych na komputerze i typów licencji:

Dyski/woluminy

Opcja dostępna, jeśli zainstalowano komponent Acronis Backup & Recovery 11 Agent for Windows lub Acronis Backup & Recovery 11 Agent for Linux.

Opcja ta służy do tworzenia kopii zapasowych całego komputera fizycznego, jego dysków lub woluminów. Aby tworzyć kopie zapasowe tych danych, musisz mieć uprawnienia administratora lub operatora kopii zapasowych.

Dzięki utworzeniu kopii zapasowej na poziomie dysku można odzyskać cały system w razie poważnego uszkodzenia danych lub awarii sprzętu. Procedura tworzenia kopii zapasowej jest szybsza niż operacja kopiowania plików, a może znacząco przyspieszyć proces tworzenia kopii zapasowej w przypadku dużych woluminów danych.

Foldery/pliki

Opcja dostępna, jeśli zainstalowano komponent Acronis Backup & Recovery 11 Agent for Windows lub Acronis Backup & Recovery 11 Agent for Linux.

Wybór tej opcji umożliwia utworzenie kopii zapasowej określonych plików i folderów.

Kopia zapasowa na poziomie pliku nie wystarcza do odzyskania systemu operacyjnego. Wybierz opcję tworzenia kopii zapasowej plików, jeśli planujesz zabezpieczenie tylko określonych danych (na przykład bieżącego projektu). Rozmiar archiwum będzie mniejszy, a więc w magazynie zostanie więcej miejsca.

Aby móc odzyskać system operacyjny z wszystkimi ustawieniami i aplikacjami, należy utworzyć kopię zapasową dysku.

Maszyny wirtualne

Opcja dostępna, jeśli zainstalowano komponent Acronis Backup & Recovery 11 Agent for ESX(i) lub Acronis Backup & Recovery 11 Agent for Hyper-V.

Opcja ta służy do tworzenia kopii zapasowych całych maszyn wirtualnych znajdujących się na serwerze wirtualizacji, ich dysków lub woluminów.

Utworzenie kopii zapasowej całej maszyny wirtualnej, jej dysków lub woluminów powoduje utworzenie standardowej kopii zapasowej dysku (s. 381). Dodatkowo w kopii zapasowej jest przechowywana konfiguracja maszyny wirtualnej. Będzie ona domyślnie sugerowana podczas odzyskiwania zawartości kopii zapasowej na nową maszynę wirtualną. Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych maszyn wirtualnych, zobacz „Tworzenie kopii zapasowych maszyn wirtualnych”.

2. W drzewie znajdującym się pod sekcją **Dane uwzględniane w kopii zapasowej** wybierz elementy do uwzględnienia w kopii zapasowej, zaznaczając znajdujące się obok pola wyboru.

Zaznaczenie pola wyboru obok komputera oznacza uwzględnienie w kopii zapasowej wszystkich jego dysków. Aby wybrać pojedyncze dyski lub woluminy, rozwiń komputer i zaznacz pola wyboru obok odpowiednich dysków lub woluminów.

Uwagi dotyczące dysków/woluminów

- Jeśli system operacyjny i jego program łądający znajdują się na różnych woluminach, w kopii zapasowej należy zawsze uwzględnić oba woluminy. Woluminy muszą być również odzyskiwane wspólnie, gdyż w przeciwnym razie istnieje duże ryzyko, że system operacyjny nie uruchomi się.
- Uwaga dla użytkowników systemu Linux: woluminy logiczne i urządzenia MD są widoczne w sekcji **Woluminy dynamiczne**. Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych takich woluminów i urządzeń, zobacz „Tworzenie kopii zapasowych oraz odzyskiwanie woluminów logicznych i urządzeń MD (Linux)” (s. 39).
- Uwaga dla użytkowników systemu Linux: Zaleca się odmontowanie wszystkich woluminów zawierających systemy plików bez funkcji księgowania — na przykład system ext2 — przed utworzeniem ich kopii zapasowej. W przeciwnym przypadku po odzyskaniu woluminy te mogą zawierać uszkodzone pliki, a odzyskiwanie ze zmianą rozmiaru może zakończyć się niepowodzeniem.

Uwagi dotyczące maszyn wirtualnych

- Tworzenie kopii zapasowych całych maszyn wirtualnych jest przydatne, gdy istnieje duża liczba małych (pod względem rozmiarów dysków wirtualnych) serwerów starszego typu, na przykład powstałych w związku z konsolidacją obciążenia. Dla każdej maszyny tworzone jest osobne archiwum.
 - Tworzenie kopii zapasowych pojedynczych dysków lub woluminów maszyny wirtualnej jest przydatne, gdy system operacyjny i aplikacje, na przykład serwer bazy danych, działają na dysku wirtualnym, ale dane, na przykład baza danych, są przechowywane na dysku fizycznym o dużej pojemności dodanym do tej samej maszyny. Można użyć różnych strategii tworzenia kopii zapasowych dysków wirtualnych i pamięci fizycznej.
3. Po określeniu danych uwzględnianych w kopii zapasowej kliknij **OK**.

4.2.2 Poświadczenia dostępu do źródła

Określ poświadczenia wymagane w celu dostępu do danych, które zostaną uwzględnione w kopii zapasowej.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
 - **Użyj poświadczeń planu**
Program uzyska dostęp do danych źródłowych przy użyciu poświadczeń konta planu tworzenia kopii zapasowych, które zostało określone w sekcji **Parametry planu**.
 - **Użyj następujących poświadczeń**
Program uzyska dostęp do danych źródłowych przy użyciu określonych poświadczeń.
Użyj tej opcji, jeśli konto planu nie posiada uprawnień dostępu do danych.
Określ:
 - **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
 - **Hasło.** Hasło dla konta.
2. Kliknij **OK**.

4.2.3 Wykluczenie plików źródłowych

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux oraz w przypadku nośników startowych.

Ta opcja dotyczy kopii zapasowych na poziomie dysków tylko z systemami plików NTFS i FAT oraz kopii zapasowych na poziomie plików we wszystkich obsługiwanych systemach plików.

Opcja określa, które pliki i foldery program ma pominąć w procesie tworzenia kopii zapasowej, a tym samym wykluczyć z listy elementów dodawanych do kopii zapasowej.

Wstępnie zdefiniowaną wartością jest: **Wyklucz pliki spełniające następujące kryteria: *.tmp, *.~, *.bak.**

Aby określić pliki i foldery do wykluczenia:

Skonfiguruj dowolne z następujących parametrów:

■ Wyklucz wszystkie ukryte pliki i foldery

Opcja ta działa tylko w systemach plików obsługiwanych przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Ukryty**. Jeśli folder jest **ukryty**, program wykluczy całą jego zawartość, w tym również pliki, które nie mają atrybutu **Ukryty**.

■ Wyklucz wszystkie pliki i foldery systemowe

Opcja ta działa tylko w systemach plików obsługiwanych przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Systemowy**. Jeśli folder jest **systemowy**, program wykluczy całą jego zawartość, w tym również pliki, które nie mają atrybutu **Systemowy**.

Atrybuty plików i folderów można sprawdzić w ich właściwościach lub używając polecenia **attrib**. Więcej informacji można znaleźć w Centrum pomocy i obsługi technicznej w systemie Windows.

■ Wyklucz pliki spełniające następujące kryteria

Zaznacz to pole wyboru, aby pominąć pliki i foldery, których nazwy pasują do podanych na liście kryteriów zwanych maskami plików. Aby utworzyć listę masek plików, użyj przycisków **Dodaj**, **Edytuj**, **Usuń** i **Usuń wszystko**.

W masce plików można użyć jednego lub kilku symboli wieloznacznych * i ?:

Gwiazdka (*) zastępuje dowolną liczbę znaków w nazwie pliku (w tym również zero). Na przykład maska Dok*.txt zwraca pliki takie jak Dok.txt i Dokument.txt.

Znak zapytania (?) zastępuje dokładnie jeden znak w nazwie pliku. Na przykład maska Dok?.txt zwraca pliki takie jak Dok1.txt i Doku.txt, ale nie zwraca plików Dok.txt ani Dok11.txt.

Aby wykluczyć folder określony przez ścieżkę zawierającą literę dysku, dodaj ukośnik odwrotny (\) do nazwy folderu w kryterium, np.: C:\Finanse\

Przykłady wykluczeń

Kryterium	Przykład	Opis
Windows i Linux		
Według nazwy	F.log	Wyklucza wszystkie pliki o nazwie „F.log”.
	F	Wyklucza wszystkie foldery o nazwie „F”.
Według maski (*)	*.log	Wyklucza wszystkie pliki z rozszerzeniem .log.
	F*	Wyklucza wszystkie pliki i foldery, których nazwa rozpoczyna się od litery „F” (np. foldery F, F1 i pliki F.log, F1.log).
Według maski (?)	F????.log	Wyklucza wszystkie pliki z rozszerzeniem .log, których nazwy składają się z czterech znaków i zaczynają od litery „F”.
Windows		
Według ścieżki pliku	C:\Finanse\F.log	Wyklucza plik „F.log” znajdujący się w folderze C:\Finanse.
Według ścieżki folderu	C:\Finanse\F\	Wyklucza folder C:\Finanse\F (należy określić pełną ścieżkę, rozpoczynającą się od litery dysku).
Linux		

Według ścieżki pliku	/home/user/Finanse/F.log	Wyklucza plik „F.log” znajdujący się w folderze /home/user/Finanse.
Według ścieżki folderu	/home/user/Finanse/	Wyklucza folder /home/user/Finanse.

Powyższe ustawienia nie dotyczą plików lub folderów jawnie wybranych do utworzenia kopii zapasowej. Przyjmijmy na przykład, że użytkownik wybrał folder MójFolder oraz plik MójPlik.tmp znajdujący się poza tym folderem, oraz określił opcję pomijania wszystkich plików .tmp. Wówczas wszystkie pliki .tmp w folderze MójFolder zostaną pominięte w procesie tworzenia kopii zapasowej, ale program nie pominie pliku MójPlik.tmp.

4.2.4 Poświadczenia dostępu do lokalizacji archiwum

Określ poświadczenia wymagane w celu uzyskania dostępu do lokalizacji archiwum kopii zapasowych. Właścicielem archiwum będzie użytkownik mający określoną nazwę.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń planu**

Program uzyska dostęp do danych źródłowych przy użyciu poświadczeń konta planu tworzenia kopii zapasowych, które zostało określone w sekcji **Parametry planu**.

- **Użyj następujących poświadczeń**

Program uzyska dostęp do danych źródłowych przy użyciu określonych poświadczeń.

Użyj tej opcji, jeśli konto planu nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.

Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Ostrzeżenie: Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejść przy użyciu programu do przechwytywania pakietów.

4.2.5 Schematy tworzenia kopii zapasowych

Wybierz jeden z dostępnych schematów tworzenia kopii zapasowych:

- **Prosty** — aby zaplanować czas i częstotliwość tworzenia kopii zapasowych danych oraz określić reguły przechowywania.
- **Uruchom teraz** — aby utworzyć kopię zapasową natychmiast po kliknięciu przycisku **OK**.
- **Dziadek-ojciec-syn** — aby użyć schematu tworzenia kopii zapasowych Dziadek-ojciec-syn. Schemat ten umożliwia tworzenie kopii zapasowej danych najwyżej raz dziennie. Użytkownik wyznacza dni wykonywania dziennej kopii zapasowej i spośród tych dni wybiera dzień tworzenia kopii tygodniowej/miesięcznej. Następnie ustawia okresy przechowywania kopii zapasowych dziennych (zwanymi „synami”), tygodniowych (zwanymi „ojcami”) i miesięcznych (zwanymi „dziadkami”). Nieaktualne kopie zapasowe będą usuwane automatycznie.

- **Wieża Hanoi** — aby użyć schematu tworzenia kopii zapasowych Wieża Hanoi. Ten schemat umożliwia planowanie czasu i częstotliwości tworzenia kopii zapasowych (sesje) oraz wybór liczby poziomów kopii (maksymalnie 16). Kopie zapasowe można wykonywać częściej niż raz dziennie. Konfigurując schemat i wybierając poziomy tworzenia kopii zapasowych, automatycznie uzyskuje się okres wycofywania, czyli gwarantowaną liczbę sesji, o którą można się cofnąć w dowolnym momencie. Mechanizm automatycznego czyszczenia umożliwia zachowanie wymaganego okresu wycofywania dzięki usuwaniu nieaktualnych kopii zapasowych i zachowywaniu najnowszych kopii na każdym poziomie.
- **Niestandardowy** — aby utworzyć schemat tworzenia kopii zapasowych, w którym użytkownik może dowolnie konfigurować strategię tworzenia kopii w sposób najlepiej odpowiadający potrzebom przedsiębiorstwa. Można zdefiniować wiele harmonogramów dla różnych typów kopii zapasowych, dodać warunki i określić reguły przechowywania.
- **Uruchamianie ręczne** — aby utworzyć zadanie tworzenia kopii zapasowej przeznaczone do ręcznego uruchamiania LUB zaplanować jednorazowe wykonanie zadania w przyszłości.
- **Pierwotna kopia zapasowa w magazynie** — aby zapisać lokalnie pełną kopię zapasową, której ostatecznym miejscem docelowym jest magazyn Acronis Online Backup Storage.

Schemat prosty

W schemacie prostym wystarczy zaplanować czas i częstotliwość tworzenia kopii zapasowej danych. Pozostałe kroki mają charakter opcjonalny.

Aby skonfigurować prosty schemat tworzenia kopii zapasowych, określ właściwe ustawienia w następujący sposób:

Harmonogram

Skonfiguruj czas i częstotliwość wykonywania kopii zapasowych danych. Aby dowiedzieć się więcej na temat konfigurowania harmonogramu, zobacz sekcję Tworzenie harmonogramu (s. 74).

Reguły przechowywania

Wybierz okres przechowywania kopii zapasowych w lokalizacji oraz określ, czy po jego upływie należy je przenieść czy usunąć. Reguły przechowywania zostaną zastosowane po utworzeniu kopii zapasowej. Domyślnie ustawiona jest opcja **Zachowuj kopie zapasowe w nieskończoność**. Oznacza ona, że kopie zapasowe nigdy nie będą usuwane automatycznie. Aby uzyskać więcej informacji na temat reguł przechowywania, zobacz Konfigurowanie reguł przechowywania kopii zapasowych (s. 93).

Typ kopii zapasowej

Aby uzyskać dostęp do tego ustawienia, kliknij **Pokaż typ kopii zapasowej, drugą lokalizację, sprawdzanie poprawności, konwersję na maszynę wirtualną**.

Wybierz typ kopii zapasowej.

- **Pełna** — wybrana domyślnie dla wszystkich lokalizacji kopii zapasowych (z wyjątkiem Acronis Online Backup Storage).
- **Przyrostowa**. Za pierwszym razem zostanie utworzona pełna kopia zapasowa. Kolejne kopie będą przyrostowe. Wybrana jako jedyny typ kopii zapasowej dla magazynu Acronis Online Backup Storage.

Uwaga: Jeśli wraz z regułami przechowywania wybrano **przyrostową** kopię zapasową, czyszczenie archiwum będzie realizowane z wykorzystaniem konsolidacji (s. 380), co zajmie dużo czasu i będzie wymagało użycia sporej ilości zasobów.

Schemat „Utwórz kopię zapasową”

W schemacie **Uruchom teraz** kopia zapasowa zostanie wykonana niezwłocznie po kliknięciu przycisku **OK** u dołu strony **Utwórz plan tworzenia kopii zapasowych**.

W polu **Typ kopii zapasowej** określ, czy utworzyć pełną, przyrostową, czy różnicową kopię zapasową (s. 34).

Schemat Dziadek-ojciec-syn

W skrócie

- Kopie zapasowe: dzienne przyrostowe („syn”), tygodniowe różnicowe („ojciec”) oraz miesięczne („dziadek”)
- Wybór dnia tworzenia tygodniowych i miesięcznych kopii zapasowych
- Wybór okresów przechowywania kopii zapasowych każdego typu

Opis

Załóżmy, że chcemy skonfigurować plan tworzenia kopii zapasowych, w ramach którego regularnie wykonywane będą dzienne (D), tygodniowe (T) i miesięczne (M) kopie zapasowe. Oto najprostszy sposób: poniższa tabela przedstawia przykładowy dwumiesięczny okres takiego planu.

	Pn	Wt	Śr	Cz	Pt	Sb	Nd
1 sty–7 sty	D	D	D	D	T	-	-
8 sty–14 sty	D	D	D	D	T	-	-
15 sty–21 sty	D	D	D	D	T	-	-
22 sty–28 sty	D	D	D	D	M	-	-
29 sty–4 lut	D	D	D	D	T	-	-
5 lut–11 lut	D	D	D	D	T	-	-
12 lut–18 lut	D	D	D	D	T	-	-
19 lut–25 lut	D	D	D	D	M	-	-
26 lut–4 mar	D	D	D	D	T	-	-

Dzienne kopie zapasowe są wykonywane każdego dnia z wyjątkiem piątku, który został wyznaczony na tworzenie tygodniowych i miesięcznych kopii zapasowych. Miesięczne kopie zapasowe są wykonywane co czwarty piątek, natomiast tygodniowe kopie zapasowe we wszystkie pozostałe piątki.

Parametry

W schemacie Dziadek-ojciec-syn (GFS) można skonfigurować poniższe parametry.

Rozpocznij tworzenie kopii zapasowej o	Określa godzinę rozpoczęcia tworzenia kopii zapasowej. Wartość domyślna to 12:00.
Utwórz kopię zapasową	Określa dni wykonywania kopii zapasowej. Wartość domyślna to dni robocze.
Co tydzień/Co miesiąc	Określa dzień spośród dni wybranych w polu Utwórz kopię zapasową dnia, który jest zarezerwowany na tworzenie tygodniowych i miesięcznych kopii zapasowych. Miesięczna kopia zapasowa będzie wykonywana co czwarty taki dzień. Wartość domyślna to piątek.

Zachowuj kopie zapasowe	<p>Określa czas przechowywania kopii zapasowych w archiwum. Czas przechowywania można określić w godzinach, dniach, miesiącach lub latach. Miesięczne kopie zapasowe można przechowywać bez ograniczeń czasowych, wybierając opcję Zachowaj w nieskończoność.</p> <p>Poniżej znajdują się wartości domyślne dla każdego typu kopii zapasowej.</p> <p>Dzienna: 5 dni (zalecane minimum)</p> <p>Tygodniowa: 7 tygodni</p> <p>Miesięczna: w nieskończoność</p> <p>Okres przechowywania tygodniowych kopii zapasowych musi być dłuższy niż okres przechowywania kopii dziennych. Okres przechowywania miesięcznych kopii zapasowych musi być dłuższy niż okres przechowywania kopii tygodniowych.</p> <p>Zaleca się przynajmniej jednotygodniowy okres przechowywania dziennych kopii zapasowych.</p>
Typ kopii zapasowej	<p>Określa typy dziennych, tygodniowych i miesięcznych kopii zapasowych</p> <ul style="list-style-type: none"> ▪ Zawsze pełna — wszystkie dzienne, tygodniowe i miesięczne kopie zapasowe będą zawsze pełne. Jest to domyślny wybór w przypadkach, gdy jako lokalizację kopii zapasowych wskazano napęd taśmowy. ▪ Pełna/Różnicowa/Przyrostowa — dzienne kopie zapasowe są przyrostowe, tygodniowe są różnicowe, a miesięczne są pełne.
Ustawienia zaawansowane	<p>Dostępne tylko w zaawansowanych wersjach programu Acronis Backup & Recovery 11 podczas tworzenia scentralizowanego planu tworzenia kopii zapasowych. Szczegółowe informacje zawiera sekcja „Zaawansowane ustawienia harmonogramu” (s. 85).</p>

Kopia zapasowa nie zostanie usunięta, dopóki nie zostaną usunięte jej wszystkie kopie zależne. Dlatego tygodniowe lub miesięczne kopie zapasowe mogą pozostawać w archiwum przez kilka dni po spodziewanej dacie utraty ważności.

Jeśli harmonogram rozpoczyna się od dziennej lub tygodniowej kopii zapasowej, zamiast niej zostanie utworzona pełna kopia zapasowa.

Przykłady

Każdy dzień ostatniego tygodnia, każdy tydzień ostatniego miesiąca

Rozważmy schemat tworzenia kopii zapasowych Dziadek-ojciec-syn, który może okazać się przydatny w wielu sytuacjach.

- Kopie zapasowe plików tworzone codziennie, w tym w sobotę i niedzielę
- Zapewnienie możliwości odzyskania plików do stanu na dowolny z ostatnich siedmiu dni
- Zapewnienie dostępu do tygodniowych kopii zapasowych ostatniego miesiąca
- Zachowywanie miesięcznych kopii zapasowych w nieskończoność

Parametry schematu tworzenia kopii zapasowych można skonfigurować w następujący sposób:

- Rozpocznij tworzenie kopii zapasowej o: **23.00**
- Utwórz kopię zapasową dnia: **Wszystkie dni**
- Tygodniowa/miesięczna: **Sobota** (przykładowo)
- Zachowuj kopie zapasowe:
 - Codzienna: **1 tydzień**

- Tygodniowa: **1 miesiąc**
- Miesięczna: **w nieskończoność**

W wyniku tych ustawień zostanie utworzone archiwum codziennych, tygodniowych i miesięcznych kopii zapasowych. Codzienne kopie zapasowe będą dostępne przez siedem dni od momentu ich utworzenia. Codzienna kopia zapasowa utworzona np. w niedzielę 1 stycznia będzie dostępna do następnej niedzieli 8 stycznia. Pierwsza tygodniowa kopia zapasowa utworzona w sobotę 7 stycznia będzie przechowywana w systemie do 7 lutego. Miesięczne kopie zapasowe nie zostaną nigdy usunięte.

Ograniczone miejsce przechowywania

Aby nie przeznaczać dużej ilości miejsca na ogromne archiwum, schemat Dziadek-ojciec-syn (GFS) można skonfigurować tak, aby krócej przechowywać kopie zapasowe, a jednocześnie zapewnić odzyskanie danych w razie ich przypadkowej utraty.

Przyjmijmy następujące założenia:

- kopie zapasowe mają być wykonywane na koniec każdego dnia roboczego;
- musi istnieć możliwość odzyskania przypadkowo usuniętego lub nieumyślnie zmodyfikowanego pliku, jeśli zostało to wykryte relatywnie szybko;
- dostęp do tygodniowej kopii zapasowej musi być zapewniony przez 10 dni od momentu jej utworzenia;
- miesięczne kopie zapasowe muszą być zachowywane przez pół roku.

Parametry schematu tworzenia kopii zapasowych można skonfigurować w następujący sposób:

- Rozpocznij tworzenie kopii zapasowej o: **18.00**
- Utwórz kopię zapasową dnia: **Dni robocze**
- Tygodniowa/miesięczna: **piątek**
- Zachowuj kopie zapasowe:
 - Codzienna: **1 tydzień**
 - Tygodniowa: **10 dni**
 - Miesięczna: **6 miesięcy**

W tym schemacie użytkownik ma tydzień na odzyskanie poprzedniej wersji uszkodzonego pliku z codziennej kopii zapasowej, a także 10-dniowy dostęp do tygodniowych kopii zapasowych. Każda miesięczna pełna kopia zapasowa będzie dostępna przez sześć miesięcy od daty jej utworzenia.

Harmonogram prac

Załóżmy, że jesteś konsultantem finansowym i pracujesz w firmie na pół etatu we wtorki i czwartki. W te dni dokonujesz zmian w dokumentach i sprawozdaniach finansowych, aktualizujesz arkusze kalkulacyjne itp. na komputerze przenośnym. Aby utworzyć kopie zapasowe tych danych możesz:

- Śledzić zmiany w sprawozdaniach finansowych, arkuszach kalkulacyjnych itp. we wtorki i czwartki (codzienna przyrostowa kopia zapasowa).
- Sporządzać tygodniowe podsumowania zmian plików w porównaniu z ostatnim miesiącem (tygodniowa różnicowa kopia zapasowa w każdy piątek).
- Raz na miesiąc robić pełną kopię zapasową plików.

Ponadto załóżmy, że chcesz zachować wszystkie kopie zapasowe — w tym dzienne — przez co najmniej sześć miesięcy.

Do tych celów odpowiedni jest następujący schemat „dziadek-ojciec-syn” (GFS):

- Rozpocznij tworzenie kopii zapasowej o: **23:30**
- Utwórz kopię zapasową dnia: **wtorek, czwartek, piątek**
- Tygodniowa/miesięczna: **piątek**
- Zachowuj kopie zapasowe:
 - Codzienna: **6 miesięcy**
 - Tygodniowa: **6 miesięcy**
 - Miesięczna: **5 lat**

W tym przykładzie codzienne przyrostowe kopie zapasowe będą wykonywane we wtorki i czwartki, natomiast kopie tygodniowe i miesięczne w piątki. Uwaga: aby wybrać **piątek** w polu **Tygodniowa/miesięczna**, trzeba najpierw zaznaczyć ten dzień w polu **Utwórz kopię zapasową dnia**.

Takie archiwum umożliwi porównanie dokumentów finansowych na pierwszy i ostatni dzień pracy oraz utworzenie pięcioletniej historii wszystkich dokumentów itp.

Bez dziennych kopii zapasowych

Przeanalizujmy bardziej egzotyczny schemat „dziadek-ojciec-syn” (GFS):

- Rozpocznij tworzenie kopii zapasowej o: **12.00 w południe**
- Utwórz kopię zapasową dnia: **piątek**
- Tygodniowa/miesięczna: **piątek**
- Zachowuj kopie zapasowe:
 - Codzienna: **1 tydzień**
 - Tygodniowa: **1 miesiąc**
 - Miesięczna: **w nieskończoność**

Zatem kopie zapasowe będą wykonywane w piątki. W ten sposób piątek będzie jedynym dniem tworzenia tygodniowych i miesięcznych kopii zapasowych, bez wyboru dnia dla kopii dziennych. Tak więc powstałe archiwum „dziadek-ojciec” będzie składać się tylko z tygodniowych kopii różnicowych i miesięcznych pełnych kopii zapasowych.

Chociaż można użyć schematu „dziadek-ojciec-syn” do utworzenia takiego archiwum, w tej sytuacji schemat niestandardowy zapewni większą elastyczność.

Niestandardowy schemat tworzenia kopii zapasowych

W skrócie

- Niestandardowy harmonogram i warunki tworzenia kopii zapasowych każdego typu
- Niestandardowy harmonogram i reguły przechowywania

Parametry

Parametr	Znaczenie
Harmonogram pełnych kopii zapasowych	Określa harmonogram i warunki wykonywania pełnej kopii zapasowej. Można na przykład tak skonfigurować tworzenie pełnej kopii zapasowej, aby była wykonywana w każdą niedzielę o 1:00 po wylogowaniu się wszystkich użytkowników.
Harmonogram przyrostowych kopii zapasowych	Określa harmonogram i warunki wykonywania przyrostowej kopii zapasowej. Jeśli w momencie uruchomienia zadania archiwum nie zawiera pełnych kopii zapasowych, zamiast kopii przyrostowej tworzona jest pełna kopia zapasowa.

Harmonogram różnicowych kopii zapasowych	<p>Określa harmonogram i warunki wykonywania różnicowej kopii zapasowej.</p> <p>Jeśli w momencie uruchomienia zadania archiwum nie zawiera pełnych kopii zapasowych, zamiast kopii różnicowej tworzona jest pełna kopia zapasowa.</p>
Czyszczenie archiwum	<p>Określa sposób usuwania starych kopii zapasowych. Dwie dostępne możliwości to regularne stosowanie reguł przechowywania (s. 94) i czyszczenie archiwum po tym, gdy w docelowej lokalizacji zabraknie miejsca.</p> <p>W domyślnej konfiguracji reguły przechowywania nie są określone. Oznacza to, że starsze kopie zapasowe nie zostaną automatycznie usunięte.</p> <p>Używanie reguł przechowywania</p> <p>Określ reguły przechowywania i warunki ich stosowania.</p> <p>To ustawienie jest zalecane dla takich lokalizacji kopii zapasowych, jak foldery współdzielone lub scentralizowane skarbce.</p> <p>Gdy w trakcie wykonywania kopii zapasowej zabraknie miejsca.</p> <p>Archiwum zostanie wyczyszczone tylko wtedy, gdy podczas tworzenia kopii zapasowej zabraknie miejsca na utworzenie nowej kopii. W takiej sytuacji program wykona następujące czynności:</p> <ul style="list-style-type: none"> ▪ Usunięcie najstarszej pełnej kopii zapasowej razem ze wszystkimi zależnymi kopiami przyrostowymi/różnicowymi. ▪ Gdy dostępna jest tylko jedna pełna kopia zapasowa, ale trwa wykonywanie pełnej kopii zapasowej, istniejąca pełna kopia zapasowa zostanie usunięta razem ze wszystkimi zależnymi kopiami przyrostowymi/różnicowymi. ▪ Gdy dostępna jest tylko jedna pełna kopia zapasowa, ale trwa wykonywanie przyrostowej lub różnicowej kopii zapasowej, zostanie wyświetlony błąd o braku dostępnego miejsca. <p>Ustawienie to jest zalecane podczas wykonywania kopii zapasowych na pamięć USB lub do strefy Acronis Secure Zone. Ustawienie to nie dotyczy skarbców zarządzanych oraz serwerów FTP i SFTP.</p> <p>Ustawienie to umożliwia usunięcie ostatniej kopii zapasowej w archiwum w sytuacji, w której urządzenie pamięci masowej nie może pomieścić więcej niż jednej kopii. Jednak jeśli program z jakiegoś powodu nie może utworzyć nowej kopii zapasowej, może to oznaczać, że nie będzie dostępna żadna kopia zapasowa.</p>
Zastosuj reguły przechowywania (tylko po skonfigurowaniu reguł przechowywania)	<p>Określa, kiedy należy zastosować reguły przechowywania (s. 94).</p> <p>Procedurę czyszczenia można na przykład skonfigurować tak, aby była uruchamiana po każdym wykonaniu kopii zapasowej, a także według harmonogramu.</p> <p>Ta opcja jest dostępna tylko pod warunkiem, że w sekcji Reguły przechowywania została skonfigurowana przynajmniej jedna reguła przechowywania.</p>
Harmonogram czyszczenia (tylko po wybraniu opcji Według harmonogramu)	<p>Określa harmonogram procedury czyszczenia archiwum.</p> <p>Rozpoczęcie czyszczenia można na przykład zaplanować na ostatni dzień każdego miesiąca.</p> <p>Ta opcja jest dostępna tylko w przypadku wybrania parametru Według harmonogramu w sekcji Zastosuj reguły przechowywania.</p>

2. lokalizacja, 3. lokalizacja itd.	<p>Określa miejsce docelowe kopiowania lub przenoszenia (s. 90) kopii zapasowych z bieżącej lokalizacji.</p> <p>Opcja ta jest dostępna pod warunkiem, że zaznaczono pole wyboru Replikuj nowo utworzoną kopię zapasową do innej lokalizacji w obszarze Sposób tworzenia kopii zapasowej lub Przenieś najstarsze kopie zapasowe do innej lokalizacji w oknie Reguły przechowywania.</p>
--	--

Przykłady

Tygodniowa pełna kopia zapasowa

Poniższy schemat umożliwia tworzenie pełnej kopii zapasowej w każdy piątek wieczorem.

Pełna kopia zapasowa: Harmonogram: Co tydzień, w każdy piątek o 22.00

W tym przykładzie pola wszystkich parametrów z wyjątkiem **Harmonogram** w **Pełna kopia zapasowa** pozostają puste. Wszystkie kopie zapasowe w archiwum są przechowywane w nieskończoność (bez czyszczenia archiwów).

Pełna i przyrostowa kopia zapasowa plus czyszczenie

W następującym schemacie archiwum zawiera tygodniowe pełne i codzienne przyrostowe kopie zapasowe. Oprócz tego wymagamy również, aby program wykonał pełną kopię zapasową tylko po wylogowaniu wszystkich użytkowników.

Pełna kopia zapasowa: Harmonogram: Co tydzień, w każdy Piątek o 22.00

Pełna kopia zapasowa: Warunki: Użytkownik wylogowany

Przyrostowa kopia zapasowa: Harmonogram: Co tydzień, w każdy dzień roboczy o 21.00

Dodatkowo ustalamy usuwanie z archiwum kopii zapasowych starszych niż jeden rok oraz wykonywanie procedury czyszczenia po utworzeniu nowej kopii zapasowej.

Reguły przechowywania: Usuwać kopie zapasowe starsze niż 12 miesięcy

Zastosuj reguły: Po wykonaniu kopii zapasowej

Domyślnie jednoroczna pełna kopia zapasowa nie zostanie usunięta, dopóki wszystkie zależne od niej przyrostowe kopie zapasowe nie zostaną również usunięte. Więcej informacji znajduje się w sekcji **Reguły przechowywania** (s. 94).

Miesięczne pełne, tygodniowe różnicowe i dzienne przyrostowe kopie zapasowe plus czyszczenie

Ten przykład pokazuje zastosowanie wszystkich dostępnych opcji w schemacie niestandardowym.

Załóżmy, że chcemy stworzyć schemat, w ramach którego będą wykonywane miesięczne pełne kopie zapasowe, tygodniowe różnicowe kopie zapasowe i dzienne przyrostowe kopie zapasowe. Wówczas harmonogram tworzenia kopii zapasowych będzie wyglądał jak poniżej.

Pełna kopia zapasowa: Harmonogram: Co miesiąc, w każdą ostatnią niedzielę miesiąca o 21.00

Przyrostowa kopia zapasowa: Harmonogram: Co tydzień, w każdy dzień roboczy o 19.00

Różnicowa kopia zapasowa: Harmonogram: Co tydzień, w każdą sobotę o 20.00

Oprócz tego chcemy dodać warunki, które muszą zostać spełnione, aby uruchomić zadanie tworzenia kopii zapasowej. Określa się je w polach **Warunki** dla każdego typu kopii zapasowej.

Pełna kopia zapasowa: Warunki: Lokalizacja jest dostępna

Przyrostowa kopia zapasowa: Warunki: Użytkownik wylogowany

Różnicowa kopia zapasowa: Warunki: Użytkownik jest bezczynny

Przy takich ustawieniach wykonanie pełnej kopii zapasowej — pierwotnie zaplanowanej na 21.00 — może faktycznie rozpocząć się później: gdy tylko będzie dostępna lokalizacja kopii zapasowej. Podobnie zadania tworzenia przyrostowych i różnicowych kopii zapasowych zostaną uruchomione dopiero, kiedy wszyscy użytkownicy odpowiednio wylogują się i będą bezczynni.

Na koniec tworzymy reguły przechowywania kopii w archiwum: zachowajmy tylko te kopie zapasowe, które nie są starsze niż sześć miesięcy i zezwólmy na wykonanie czyszczenia po każdym zadaniu tworzenia kopii zapasowej oraz również ostatniego dnia każdego miesiąca.

Reguły przechowywania: Usuwać kopie zapasowe starsze niż **6 miesięcy**

Zastosuj reguły: After backing up (Po utworzeniu kopii zapasowej), Według harmonogramu

Harmonogram czyszczenia: Co miesiąc, Ostatni dzień, Wszystkie miesiące, o 22.00

Domyślnie program nie usuwa kopii zapasowej, dopóki istnieją zależne kopie zapasowe, które muszą zostać zachowane. Jeżeli na przykład pełna kopia zapasowa przeznaczona do usunięcia posiada zależne kopie przyrostowe lub różnicowe, usunięcie zostanie odłożone do momentu, kiedy będzie można usunąć również kopie zależne.

Więcej informacji znajduje się w części Reguły przechowywania (s. 94).

Schemat Wieża Hanoi

W skrócie

- Maksymalnie 16 poziomów pełnych, różnicowych i przyrostowych kopii zapasowych.
- Kopie zapasowe kolejnego poziomu występują dwa razy rzadziej niż kopie zapasowe poprzedniego poziomu.
- Jednocześnie jest przechowywana tylko jedna kopia zapasowa każdego poziomu.
- Większe zagęszczenie nowszych kopii zapasowych.

Parametry

Można skonfigurować następujące parametry schematu Wieża Hanoi:

Harmonogram	Skonfiguruj harmonogram dzienny (s. 76), tygodniowy (s. 78) lub miesięczny (s. 80). Konfiguracja parametrów harmonogramu umożliwia tworzenie harmonogramów prostych (przykład prostego harmonogramu dziennego: zadanie tworzenia kopii zapasowej uruchamiane codziennie o 10:00) oraz harmonogramów bardziej złożonych (przykład złożonego harmonogramu dziennego: zadanie uruchamiane co trzy dni, począwszy od 15 stycznia, oraz powtarzane w określone dni co dwie godziny od 10:00 do 22:00). W ten sposób złożony harmonogram określa sesje, podczas których schemat ma być stosowany. W poniższym omówieniu termin „dni” można zastąpić terminem „zaplanowane sesje”.
Liczba poziomów	Wybierz od 2 do 16 poziomów tworzenia kopii zapasowych. Zobacz szczegółowy przykład poniżej.
Okres wycofywania	Gwarantowana liczba sesji, o którą w dowolnym momencie można cofnąć się w archiwum. Obliczana jest automatycznie na podstawie wybranych parametrów harmonogramu i liczby poziomów. Zobacz szczegółowy przykład poniżej.

Typ kopii zapasowej	<p>określa typy kopii zapasowej, które będą przypisane do poziomów kopii zapasowej</p> <ul style="list-style-type: none"> ▪ Zawsze pełna — wszystkie poziomy kopii zapasowej będą pełne. Jest to domyślny wybór w przypadkach, gdy jako lokalizację kopii zapasowych wskazano napęd taśmowy. ▪ Pełna/różnicowa/przyrostowa — kopie zapasowe na różnych poziomach będą się różniły typem: <ul style="list-style-type: none"> - Kopie zapasowe ostatniego poziomu to kopie pełne - Kopie zapasowe poziomów pośrednich to kopie różnicowe - Kopie zapasowe pierwszego poziomu to kopie przyrostowe
----------------------------	---

Przykład

Parametry **harmonogramu** są następujące:

- Powtarzaj co: 1 dzień
- Częstotliwość: Raz o 18.00

Liczba poziomów: 4

Typ kopii zapasowej: Pełna/różnicowa/przyrostowa

Poniżej przedstawiono wygląd pierwszych 14 dni (czyli 14 sesji) harmonogramu według tego schematu. Liczby zaciemnione oznaczają poziom tworzenia kopii zapasowych.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Kopie zapasowe różnych poziomów są różnego typu:

- Kopie zapasowe *ostatniego poziomu* (w tym przypadku poziomu 4) to kopie pełne.
- Kopie zapasowe *poziomów pośrednich* (2, 3) to kopie różnicowe.
- Kopie zapasowe **pierwszego poziomu** (1) to kopie przyrostowe.

Zastosowanie mechanizmu czyszczenia umożliwia zachowanie tylko najnowszych kopii zapasowych każdego poziomu. W dniu 8 — dzień przed utworzeniem nowej pełnej kopii zapasowej — archiwum będzie wyglądać jak poniżej.

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

Ten schemat zapewnia efektywne wykorzystanie pamięci masowej, ponieważ im bardziej aktualne dane, tym większa liczba kopii zapasowych. W przypadku czterech kopii zapasowych można odzyskać dane z bieżącego dnia, z poprzedniego dnia, sprzed połowy tygodnia i sprzed tygodnia.

Okres wycofywania

Liczba dni, o którą można cofnąć się w archiwum, jest inna w różne dni. Minimalna gwarantowana liczba dni nosi nazwę okresu wycofywania.

Tabela poniżej pokazuje okresy tworzenia i wycofywania kopii zapasowych dla schematów z różnymi poziomami.

Liczba poziomów	Pełna kopia zapasowa co	W zależności od dnia można powrócić	Okres wycofywania
2	2 dni	od 1 do 2 dni	1 dzień
3	4 dni	od 2 do 5 dni	2 dni
4	8 dni	od 4 do 11 dni	4 dni
5	16 dni	od 8 do 23 dni	8 dni
6	32 dni	od 16 do 47 dni	16 dni

Dodanie poziomu powoduje podwojenie okresów tworzenia pełnej kopii zapasowej oraz wycofywania.

Wróćmy do poprzedniego przykładu, aby zobaczyć, dlaczego liczba dni odzyskiwania się zmienia.

Oto kopie zapasowe w dniu 12 (liczby w kolorze szarym oznaczają usunięte kopie zapasowe).

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

Nowa różnicowa kopia zapasowa na poziomie 3 jeszcze nie została utworzona, zatem nadal przechowywana jest kopia z dnia 5. Ponieważ jest ona zależna od pełnej kopii zapasowej z dnia 1, kopia pełna również jest dostępna. Dzięki temu można cofnąć się aż o 11 dni, co jest scenariuszem najbardziej optymistycznym.

Jednak w następnym dniu zostanie utworzona nowa różnicowa kopia zapasowa trzeciego poziomu, a stara pełna kopia zapasowa zostanie usunięta.

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

To daje zaledwie czterodniowy okres na odzyskiwanie danych, co okazuje się być najgorszym scenariuszem w tym przypadku.

W dniu 14 przedział ten wynosi pięć dni. W kolejne dni przedział się wydłuża, następnie ponownie się skraca itd.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Okres wycofywania wskazuje gwarantowaną liczbę dni dostępną nawet w najbardziej pesymistycznym przypadku. Przy schemacie z czterema poziomami wynosi on cztery dni.

Uruchamianie ręczne

Schemat **Uruchamianie ręczne** nie wymaga określania harmonogramu tworzenia kopii zapasowych. Plan tworzenia kopii zapasowych można będzie później w dowolnym momencie uruchomić ręcznie z poziomu widoku **Plany i zadania**.

Określ odpowiednie ustawienia w poniższy sposób.

Typ kopii zapasowej

Wybierz typ kopii zapasowej

- **Pełna** — wybrana domyślnie dla wszystkich lokalizacji kopii zapasowych (z wyjątkiem Acronis Online Backup Storage).
- **Przyrostowa**. Za pierwszym razem zostanie utworzona pełna kopia zapasowa. Kolejne kopie będą przyrostowe. Wybrana jako jedyny typ kopii zapasowej dla magazynu Acronis Online Backup Storage.
- **Różnicowa** Za pierwszym razem zostanie utworzona pełna kopia zapasowa. Kolejne kopie będą różnicowe.

4.2.6 Wybór lokalizacji kopii zapasowej

Określ miejsce przechowywania archiwum.

1. Wybieranie lokalizacji docelowej

Wprowadź pełną ścieżkę do miejsca docelowego w polu **Ścieżka** lub wybierz miejsce docelowe w drzewie lokalizacji zgodnie z opisem w sekcji „Wybór miejsc docelowych kopii zapasowych” (s. 66).

2. Korzystanie z tabeli archiwów

Aby ułatwić wybranie właściwego miejsca docelowego, w tabeli przedstawione są nazwy archiwów znajdujących się we wszystkich wybranych lokalizacjach. Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

3. Nadawanie nazwy nowemu archiwum

Po wybraniu docelowego miejsca archiwum program generuje nazwę nowego archiwum i wyświetla ją w polu **Nazwa**. Nazwa ma zwykle postać *Archiwum(N)*, gdzie *N* to numer kolejnego archiwum. Wygenerowana nazwa jest unikatowa dla wybranej lokalizacji. Jeśli nazwa wygenerowana automatycznie jest zadowalająca, kliknij **OK**. W przeciwnym razie wprowadź inną unikatową nazwę.

Jeśli nazwa wygenerowana automatycznie wygląda tak: *[Nazwa maszyny]_Archiwum(N)*, oznacza to, że zawiera zmienne. Taka sytuacja może wystąpić, jeśli użytkownik wybrał tworzenie kopii zapasowych danych maszyn wirtualnych. *[Nazwa maszyny]* oznacza nazwę maszyny wirtualnej. Do nazw można dodać sufiksy, ale nigdy nie wolno usuwać zmiennych, ponieważ dane każdej maszyny wirtualnej muszą być kopiowane do oddzielnego archiwum z unikatową nazwą.

Tworzenie kopii zapasowej w istniejącym archiwum

Plan tworzenia kopii zapasowych można skonfigurować tak, aby kopie tworzone były w istniejącym archiwum. W tym celu wybierz archiwum w tabeli archiwów lub wpisz jego nazwę w polu **Nazwa**. Jeśli archiwum jest chronione hasłem, użytkownik zostanie poproszony o podane hasła w oknie wyskakującym.

Wybierając istniejące archiwum, użytkownik ingeruje w obszar innego planu tworzenia kopii zapasowych, który korzysta z tego samego archiwum. Nie jest to problem, jeśli ten drugi plan ma zostać wycofany. Ogólnie jednak należy przestrzegać zasady: „jeden plan tworzenia kopii zapasowych — jedno archiwum”. Działanie niezgodne z tą zasadą nie spowoduje zatrzymania programu, ale nie jest ono ani praktyczne, ani wydajne, z wyjątkiem niektórych szczególnych przypadków.

Dlaczego nie należy tworzyć kopii zapasowych dwóch lub więcej planów w tym samym archiwum

1. Tworzenie kopii zapasowych różnych źródeł w tym samym archiwum utrudnia korzystanie z takiego archiwum. W przypadku odzyskiwania danych liczy się każda sekunda, a w archiwum o takiej zawartości można się zgubić.








Plany tworzenia kopii zapasowych korzystające z tego samego archiwum powinny uwzględniać w kopii zapasowej identyczne elementy danych (na przykład wolumin C).





2. Stosowanie wielu reguł przechowywania w archiwum sprawia, że w pewien sposób zawartość takiego archiwum trudno jest przewidzieć. Reguły zostaną zastosowane do całego archiwum, dlatego kopie zapasowe należące do jednego planu tworzenia kopii zapasowych mogą być łatwo usunięte razem z kopiami zapasowymi należącymi do innego planu. Może to być szczególnie widoczne w schematach tworzenia kopii zapasowych dziadek-ojciec-syn oraz Wieża Hanoi.

Zwykle dla każdego złożonego planu tworzenia kopii zapasowych istnieje oddzielne archiwum.

Wybór docelowych lokalizacji kopii zapasowych

Program Acronis Backup & Recovery 11 umożliwia tworzenie kopii zapasowych w różnych fizycznych urządzeniach pamięci masowej.

Miejsce docelowe	Szczegóły
 Magazyn kopii zapasowych online	<p>Aby utworzyć kopię zapasową danych w magazynie Acronis Online Backup Storage, kliknij Zaloguj i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę Magazyn kopii zapasowych online i wybierz konto.</p> <p>Przed utworzeniem kopii zapasowej w magazynie online należy zakupić subskrypcję usługi tworzenia kopii zapasowych online oraz aktywować tę subskrypcję na komputerach, których kopię zapasową chcesz utworzyć.</p> <p>Opcja tworzenia kopii zapasowej online jest niedostępna w systemie Linux i podczas pracy z nośnikiem startowym.</p> <hr/> <p>Uwaga: Usługa Acronis Backup & Recovery Online nie jest dostępna we wszystkich regionach. Aby uzyskać więcej informacji, kliknij tutaj: http://www.acronis.pl/my/backup-recovery-online/.</p>
 Osobisty	<p>Aby utworzyć kopię zapasową danych w skarbcu osobistym, rozwiń grupę Skarbcze i kliknij skarbiec.</p> <p>Strefa Acronis Secure Zone jest obsługiwana jako skarbiec osobisty dostępny dla wszystkich użytkowników, którzy mogą się zalogować do systemu.</p>
 Centralny	<p>Aby utworzyć kopię zapasową danych w skarbcu centralnym, rozwiń grupę Skarbcze i kliknij skarbiec.</p>
 Komputer	Komputer lokalny
 Foldery lokalne	<p>Aby utworzyć kopię zapasową danych w folderach lokalnych komputera, rozwiń grupę <Nazwa komputera> i wybierz żądany folder.</p>
 CD, DVD itp.	<p>Aby utworzyć kopię zapasową danych na nośnikach optycznych takich jak CD lub DVD, rozwiń grupę <Nazwa komputera> i wybierz żądany napęd.</p>
 Urządzenie taśmowe	<p>Aby utworzyć kopię danych w lokalnie podłączonym urządzeniu taśmowym, rozwiń grupę <Nazwa komputera>, a następnie kliknij żądane urządzenie.</p> <p>W autonomicznych wersjach programu Acronis Backup & Recovery 11 urządzenia taśmowe są dostępne tylko w przypadku aktualizacji z wersji Acronis Backup & Recovery 10. Aby uzyskać więcej informacji na temat używania taśm, zobacz sekcję „Urządzenia taśmowe” (s. 191).</p>

Miejsce docelowe	Szczegóły
 Foldery sieciowe	<p>Aby utworzyć kopię zapasową danych w folderze sieciowym, rozwiń grupę Foldery sieciowe, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony.</p> <p>Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.</p> <hr/> <p>Uwaga dla użytkowników systemu Linux: Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak <code>/mnt/share</code>, należy wybrać ten punkt montowania, a nie sam udział sieciowy.</p>
 FTP, SFTP	<p>Aby utworzyć kopię zapasową danych na serwerze FTP lub SFTP, wpisz nazwę i adres serwera w polu Ścieżka w następujący sposób:</p> <p>ftp://serwer_ftp:numer_portu lub sftp://serwer_sftp:numer_portu</p> <p>Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.</p> <p>Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder.</p> <p>Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję Użyj dostępu anonimowego.</p> <hr/> <p>Uwaga: Zgodnie z oryginalną specyfikacją protokołu FTP poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako zwykły tekst. Oznacza to, że nazwę użytkownika i hasło można przechwycić przy użyciu programu do przechwytywania pakietów.</p>
 Węzły magazynowania	<p>Jeśli musisz utworzyć kopię zapasową danych w węźle magazynowania niezarejestrowanym na serwerze zarządzania lub działającym na komputerze uruchomionym za pomocą nośnika startowego:</p> <ul style="list-style-type: none"> Aby uzyskać dostęp do skarbca zarządzanego, w polu Ścieżka wpisz następujący ciąg: bsp://adres_węzła/nazwa_skarbca/ Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.
 Dyski NFS	<p>Aby utworzyć kopię zapasową danych w udziale NFS, rozwiń grupę Dyski NFS i kliknij folder.</p> <p>Możliwość ta jest dostępna tylko w systemie Linux i po uruchomieniu komputera za pomocą nośnika startowego opartego na systemie Linux.</p>

4.2.7 Sprawdzanie poprawności archiwum

Należy skonfigurować zadanie sprawdzania poprawności, aby sprawdzić możliwość odzyskania danych z kopii zapasowych. Jeśli proces sprawdzania poprawności kopii zapasowej nie zakończy się pomyślnie, zadanie sprawdzania poprawności zakończy się niepowodzeniem, a plan tworzenia kopii zapasowych otrzyma status Błąd.

Aby skonfigurować sprawdzanie poprawności, określ następujące parametry

1. **Czas sprawdzania poprawności** — wybierz czas wykonywania zadania sprawdzania poprawności. Sprawdzanie poprawności to operacja intensywnie korzystająca z zasobów i zaleca się

zaplanowanie sprawdzania poprawności na komputerze zarządzanym poza okresem największego ruchu. Jednak jeśli sprawdzanie poprawności stanowi zasadniczą część strategii ochrony danych i użytkownik chce niezwłocznie wiedzieć, czy dane kopii zapasowej są uszkodzone i czy można je pomyślnie odzyskać, warto rozważyć rozpoczęcie sprawdzania poprawności natychmiast po utworzeniu kopii zapasowej.

2. **Elementy do sprawdzenia poprawności** — wybierz sprawdzanie poprawności całego archiwum lub ostatniej kopii zapasowej w tym archiwum. Sprawdzanie poprawności kopii zapasowej plików symuluje odzyskiwanie wszystkich plików z kopii zapasowej do tymczasowego miejsca docelowego. Sprawdzanie poprawności kopii zapasowej woluminu polega na obliczeniu sumy kontrolnej wszystkich bloków danych zapisanych w kopii zapasowej. Sprawdzanie poprawności archiwum oznacza sprawdzenie poprawności wszystkich kopii zapasowych tego archiwum i może zająć dużo czasu oraz korzystać z dużej ilości zasobów systemu.
3. **Harmonogram sprawdzania poprawności** (pojawia się wyłącznie po wybraniu opcji Według harmonogramu w kroku 1) — określ harmonogram sprawdzania poprawności. Więcej informacji znajduje się w sekcji Tworzenie harmonogramu (s. 74).

4.2.8 Poświadczenia planu tworzenia kopii zapasowych

Podaj poświadczenia konta, na którym zadania planu będą wykonywane.

Aby określić poświadczenia

1. Wybierz jedno z następujących ustawień:

- **Użyj poświadczeń bieżącego użytkownika**

Zadania będą uruchamiane przy użyciu poświadczeń, z którymi zalogował się użytkownik rozpoczynający zadania. Jeśli jedno z zadań ma zostać wykonane według harmonogramu, w momencie zakończenia tworzenia planu użytkownik zostanie poproszony o aktualne hasło użytkownika.

- **Użyj następujących poświadczeń**

Zadania będą zawsze uruchamiane przy użyciu poświadczeń określonych przez użytkownika, niezależnie od tego, czy zadanie będzie uruchamiane ręcznie, czy wykonywane według harmonogramu.

Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Aby dowiedzieć się więcej na temat operacji użytkowników z różnymi uprawnieniami, zobacz sekcję Uprawnienia użytkowników na zarządzanym komputerze (s. 33).

4.2.9 Etykieta (zachowanie właściwości komputera w kopii zapasowej)

Podczas każdego tworzenia kopii zapasowej danych na komputerze do kopii zapasowej są dołączane informacje na temat nazwy komputera, systemu operacyjnego, pakietu Service Pack systemu Windows i identyfikatora zabezpieczeń (SID) oraz etykieta tekstowa zdefiniowana przez użytkownika. Etykieta może zawierać nazwę działu lub nazwisko właściciela komputera, albo podobne informacje, których można użyć jako znacznika lub klucza.

W przypadku odzyskiwania (s. 130) komputera na serwer VMware ESX(i) przy użyciu agenta dla ESX(i) albo konwertowania (s. 99) kopii zapasowej na maszynę wirtualną ESX(i) te właściwości zostaną przeniesione do konfiguracji maszyny wirtualnej. Możesz je wyświetlić w ustawieniach maszyny wirtualnej: **Edytuj ustawienia > Opcje > Zaawansowane > Ogólne > Parametry konfiguracji**. Przy użyciu tych niestandardowych parametrów możesz wybierać, sortować i łączyć w grupy maszyny wirtualne. Może to być przydatne w różnych scenariuszach.

Przykład:

Przyjmijmy, że migrujesz swoje biuro lub centrum danych do środowiska wirtualnego. Przy użyciu oprogramowania innych firm, które może uzyskiwać dostęp do parametrów konfiguracji przy użyciu interfejsu VMware API, możesz automatycznie stosować zasady zabezpieczeń na każdym komputerze, nawet przed jego włączeniem.

Aby dodać etykietę tekstową do kopii zapasowej:

1. Na stronie **Utwórz plan tworzenia kopii zapasowych** (s. 48) kliknij **Pokaż poświadczenia, komentarze, etykietę planu**.
2. W polu **Etykieta** wprowadź etykietę tekstową lub wybierz ją z menu rozwijanego.

Omówienie parametrów

Parametr	Wartość	Opis
acronisTag.label	<string>	Etykieta zdefiniowana przez użytkownika. Etykietę może ustawić użytkownik podczas tworzenia planu tworzenia kopii zapasowych.
acronisTag.hostname	<string>	Nazwa hosta (w pełni kwalifikowana nazwa domeny, FQDN)
acronisTag.os.type	<string>	System operacyjny,
acronisTag.os.servicepack	0, 1, 2...	Wersja dodatku Service Pack zainstalowanego w systemie. Tylko dla systemu operacyjnego Windows.
acronisTag.os.sid	<string>	Identyfikator zabezpieczeń (SID) komputera Na przykład: S-1-5-21-874133492-782267321-3928949834. Tylko dla systemu operacyjnego Windows.

Wartości parametru „acronisTag.os.type”

Windows NT 4	winNTGuest
Windows 2000 Professional	win2000ProGuest
Windows 2000 Server	win2000ServGuest
Windows 2000 Advanced Server	win2000ServGuest
Windows XP — wszystkie wersje	winXPProGuest
Windows XP — wszystkie wersje (64-bitowe)	winXPPro64Guest
Windows Server 2003 — wszystkie wersje	winNetStandardGuest
Windows Server 2003 — wszystkie wersje (64-bitowe)	winNetStandard64Guest
Windows 2008	winLonghornGuest
Windows 2008 (64-bitowy)	winLonghorn64Guest
Windows Vista	winVistaGuest
Windows Vista (64-bitowy)	winVista64Guest

Windows 7	windows7Guest
Windows 7 (64-bitowy)	windows7_64Guest
Windows Server 2008 R2 (64-bitowy)	windows7Server64Guest
Linux	otherLinuxGuest
Linux (64-bitowy)	otherLinux64Guest
Inny system operacyjny	otherGuest
Inny system operacyjny (64-bitowy)	otherGuest64

Przykład

```

acronisTag.label = "DEPT:BUCH; COMP:SUPERSEVER; OWNER:EJONSON"
acronisTag.hostname = "superserver.corp.local"
acronisTag.os.type = "windows7Server64Guest"
acronisTag.os.servicepack = "1"
acronisTag.os.sid = "S-1-5-21-874133492-782267321-3928949834"

```

4.2.10 Dlaczego program wyświetla monit o hasło?

Zaplanowane lub przełożone zadanie musi zostać uruchomione niezależnie od zalogowanych użytkowników. W sytuacji, gdy nie określono wprost poświadczeń, z którymi zadania mają zostać uruchomione, program proponuje użycie konta użytkownika. Wprowadź hasło użytkownika, określ inne konto lub zmień typ zaplanowanego uruchomienia na ręczny.

4.3 Uprozczone nazewnictwo plików kopii zapasowych

Tworząc plan tworzenia kopii zapasowych (s. 48), możesz wybrać standardowe lub uproszczone nazewnictwo plików kopii.

Jeśli zaznaczysz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**:

- Nazwa pliku pierwszej (pełnej) kopii zapasowej w archiwum będzie zawierała nazwę archiwum, na przykład: **MojeDane.tib**. Nazwy plików kolejnych (przyrostowych lub różnicowych) kopii zapasowych będą zawierać indeks. Na przykład: **MojeDane2.tib**, **MojeDane3.tib** itd.

Ten prosty schemat nazewnictwa umożliwia utworzenie przenośnego obrazu komputera na nośniku wymiennym lub przeniesienie kopii zapasowych do innej lokalizacji przy użyciu skryptu.

- Przed utworzeniem nowej pełnej kopii zapasowej program usuwa całe archiwum i zakłada nowe. Jest to istotne w sytuacji, gdy używane są wymienne dyski twarde USB, a na każdym z nich ma się znajdować jedna pełna kopia zapasowa (s. 72) lub wszystkie kopie zapasowe utworzone w danym tygodniu (s. 72). Może jednak zdarzyć się, że nie zostanie utworzona żadna kopia zapasowa, gdy nie powiedzie się utworzenie pełnej kopii zapasowej na jedyńm dysku.

Ten sposób działania można ograniczyć, dodając do nazwy archiwum zmienną [Date] (s. 74).

Jeśli *nie* zaznaczysz pola wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**:

- Każda kopia zapasowa będzie miała unikatową nazwę pliku zawierającą dokładny znacznik czasu oraz typ kopii zapasowej. Na przykład: **MojeDane_2010_03_26_17_01_38_960D.tib**. Ten standard nazewnictwa umożliwia używanie szerszego zakresu lokalizacji docelowych kopii zapasowych oraz schematów tworzenia kopii zapasowych.

Ograniczenia

W przypadku używania uproszczonego nazewnictwa plików następujące funkcje są niedostępne:

- Konfigurowanie tworzenia pełnych, przyrostowych i różnicowych kopii zapasowych w jednym planie tworzenia kopii zapasowych. Trzeba utworzyć oddzielne plany tworzenia kopii zapasowych dla każdego z typów kopii.
- Tworzenie kopii zapasowych w skarbcu zarządzanym, na taśmie, w strefie Acronis Secure Zone lub w magazynie Acronis Online Backup Storage
- Konfigurowanie reguł przechowywania
- Konfigurowanie regularnej konwersji kopii zapasowych na maszynę wirtualną

Wskazówka. Systemy plików FAT16, FAT32 oraz NTFS nie pozwalają na używanie następujących znaków w nazwach plików: ukośnika odwrotnego (\), ukośnika (/), dwukropka (:), gwiazdki (*), pyłajnika (?), cudzysłowu ("), znaku mniejszości (<), znaku większości (>), oraz kreski pionowej (|).

4.3.1 Przykłady użycia

W tej sekcji przedstawiono przykłady użycia uproszczonego nazewnictwa plików.

Przykład 1. Codzienna kopia zapasowa zastępująca starą kopię

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć pełną kopię zapasową swojego komputera.
- Chcesz zapisać kopię zapasową lokalnie, w pliku **MójKomputer.tib**.
- Chcesz, aby każda nowa kopia zapasowa zastępowała starą kopię.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych zawierający codzienny harmonogram. Podczas tworzenia planu tworzenia kopii zapasowych jako nazwę archiwum określ **MójKomputer**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, a następnie wybierz typ kopii zapasowej **Pełna**.

Rezultat. Archiwum składa się z jednego pliku: **MójKomputer.tib**. Plik jest usuwany przed utworzeniem nowej kopii zapasowej.

Przykład 2. Codzienne pełne kopie zapasowe ze znacznikiem daty

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć pełną kopię zapasową swojego komputera.
- Chcesz przenosić stare kopie zapasowe do zdalnej lokalizacji przy użyciu skryptu.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych zawierający codzienny harmonogram. Podczas tworzenia planu tworzenia kopii zapasowych jako nazwę archiwum określ **MójKomputer-[DATE]**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, a następnie wybierz typ kopii zapasowej **Pełna**.

Rezultat:

- Kopie zapasowe z dnia 1 stycznia 2011 r., 2 stycznia 2011 r. itd. będą zapisywane odpowiednio w plikach **MójKomputer-1.1.2011.tib**, **MójKomputer-1.2.2011.tib** itd.
- Twój skrypt może przenosić stare kopie zapasowe na podstawie znacznika daty.

Zobacz także „Zmienna [Date]” (s. 74).

Przykład 3. Kopie zapasowe tworzone co godzinę w ciągu dnia

Rozważmy następujący scenariusz:

- Chcesz codziennie co godzinę tworzyć kopie zapasowe najważniejszych plików serwera.
- Chcesz, aby pierwsza kopia zapasowa była tworzona każdego dnia o północy i była pełna, a kolejne kopie zapasowe w danym dniu były różnicowe, a ich tworzenie było uruchamiane o godzinie 01:00, 02:00 itd.
- Chcesz zachować starsze kopie zapasowe w archiwum.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych zawierający codzienny harmonogram. Podczas tworzenia planu tworzenia kopii zapasowych jako nazwę archiwum określ **PlikiSerwera([Date])**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, jako typ kopii zapasowej wybierz **Różnicowa**, a następnie zaplanuj tworzenie kopii zapasowych co godzinę od północy.

Rezultat:

- 24 kopie zapasowe z dnia 1 stycznia 2011 r. zostaną zapisane jako Pliki serwera(1.1.2011).tib, PlikiSerwera(1.1.2011)2.tib itd., aż do PlikiSerwera(1.1.2011)24.tib.
- Kolejnego dnia tworzenie kopii zapasowych rozpocznie się od pełnej kopii zapasowej PlikiSerwera(1.2.2011).tib.

Zobacz także „Zmienna [Date]” (s. 74).

Przykład 4. Codzienne pełne kopie zapasowe z codzienną zamianą dysków

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć pełne kopie zapasowe komputera w pliku **MójKomputer.tib** na zewnętrznym dysku twardym.
- Masz dwa takie dyski. Do każdego z nich po podłączeniu do komputera jest przypisywana litera dysku **D**.
- Chcesz zamieniać dyski przed każdym utworzeniem kopii zapasowej, tak aby jeden dysk zawierał dzisiejszą kopię zapasową, a drugi wczorajszą kopię zapasową.
- Chcesz, aby każda nowa kopia zapasowa zastępowała kopię znajdującą się na aktualnie podłączonym dysku.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych zawierający codzienny harmonogram. Podczas tworzenia planu tworzenia kopii zapasowych jako nazwę archiwum określ **MójKomputer**, a jako lokalizację archiwum określ **D:**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, a następnie wybierz typ kopii zapasowej **Pełna**.

Rezultat. Każdy z dysków twardych będzie zawierał jedną pełną kopię zapasową. Gdy jeden z dysków jest podłączony do komputera, drugi z nich możesz przechowywać w innej lokalizacji w celu zapewnienia dodatkowej ochrony danych.

Przykład 5. Codzienne kopie zapasowe z cotygodniową zamianą dysków

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć kopie zapasowe komputera: pełną kopię zapasową w każdy poniedziałek, oraz przyrostowe kopie zapasowe od wtorku do niedzieli.
- Chcesz tworzyć kopię zapasową w archiwum **MójKomputer** na zewnętrznym dysku twardym.
- Masz dwa takie dyski. Do każdego z nich po podłączeniu do komputera w systemie operacyjnym jest przypisywana litera dysku **D**.

- Chcesz zamieniać dyski w każdy poniedziałek, tak aby jeden z nich zawierał kopie zapasowe z bieżącego tygodnia (od poniedziałku do niedzieli), a drugi kopie z poprzedniego tygodnia.

W tym scenariuszu musisz utworzyć dwa następujące plany tworzenia kopii zapasowych:

- Podczas tworzenia pierwszego planu tworzenia kopii zapasowych jako nazwę archiwum określ **MójKomputer**, a jako lokalizację archiwum określ **D:**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, a następnie wybierz typ kopii zapasowej **Pełna** i zaplanuj uruchamianie tworzenia kopii zapasowych co tydzień w poniedziałek.
- Podczas tworzenia drugiego planu tworzenia kopii zapasowych określ te same ustawienia, ale wybierz typ kopii zapasowej **Przyrostowa** i zaplanuj tworzenie kopii zapasowych co tydzień od wtorku do niedzieli.

Rezultat:

- Przed utworzeniem kopii zapasowej w poniedziałek (według pierwszego planu tworzenia kopii zapasowych) wszystkie kopie zapasowe zostaną usunięte z aktualnie podłączonego dysku.
- Gdy jeden z dysków jest podłączony do komputera, drugi z nich możesz przechowywać w innej lokalizacji w celu zapewnienia dodatkowej ochrony danych.

Przykład 6. Kopie zapasowe w godzinach pracy

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć kopie zapasowe najważniejszych plików serwera.
- Chcesz codziennie tworzyć pełną kopię zapasową o godzinie 01:00.
- Chcesz tworzyć różnicowe kopie zapasowe w godzinach pracy, od 8:00 do 17:00.
- Chcesz do nazwy każdego pliku kopii zapasowej dołączyć datę jej utworzenia.

W tym scenariuszu musisz utworzyć dwa następujące plany tworzenia kopii zapasowych:

- Podczas tworzenia pierwszego planu tworzenia kopii zapasowych jako nazwę archiwum określ **PlikiSerwera([DATE])**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, jako typ kopii zapasowej wybierz **Pełna**, a następnie zaplanuj tworzenie kopii zapasowych codziennie o godz. 01:00:00.
- Podczas tworzenia drugiego planu tworzenia kopii zapasowych określ te same ustawienia, jak dla pierwszego planu, ale wybierz typ kopii zapasowej **Różnicowa** i zaplanuj tworzenie kopii zapasowych w następujący sposób:
 - **Uruchom zadanie: Codziennie**
 - **Co: 1 godz.**
 - **Od: 08:00:00**
 - **Do: 17:01:00**

Rezultat:

- Pełna kopia zapasowa z dnia 31 stycznia 2011 r. zostanie zapisana pod nazwą **PlikiSerwera(1.31.2011).tib**.
- 10 różnicowych kopii zapasowych z dnia 31 stycznia 2011 r. zostanie zapisanych pod nazwami **PlikiSerwera(1.31.2011)2.tib**, **PlikiSerwera(1.31.2011)3.tib** itd., aż do **PlikiSerwera(1.31.2011)11.tib**.
- Kolejnego dnia, 1 lutego 2011 r., tworzenie kopii zapasowych rozpocznie się od pełnej kopii zapasowej **PlikiSerwera(2.1.2011).tib**. Różnicowe kopie zapasowe będą się rozpoczynały od pliku **PlikiSerwera(2.1.2011)2.tib**.

Zobacz także „Zmienna [Date]” (s. 74).

4.3.2 Zmienna [DATE]

Jeśli w nazwie archiwum określisz zmienną **[DATE]**, do nazwy pliku każdej kopii zapasowej program dołączy datę utworzenia tej kopii.

W przypadku użycia tej zmiennej pierwsza kopia zapasowa utworzona danego dnia będzie pełną kopią zapasową. Przed utworzeniem kolejnej pełnej kopii zapasowej program usunie wszystkie kopie zapasowe utworzone wcześniej tego samego dnia. Kopie zapasowe utworzone w poprzednich dniach zostaną zachowane. Oznacza to, że możesz zapisać kilka pełnych kopii zapasowych wraz z kopiami przyrostowymi lub bez nich, ale nie więcej niż jedną pełną kopię zapasową dziennie. Kopie zapasowe możesz sortować według daty, kopiować, przenosić, usuwać ręcznie lub przy użyciu skryptu.

Format daty to: *m.d.rrrr*. Na przykład 1.31.2011 oznacza 31 stycznia 2011 roku. (Nie występują zera wiodące).

Możesz umieścić tę zmienną w dowolnym miejscu w nazwie archiwum. W tej zmiennej możesz użyć zarówno wielkich, jak i małych liter.

Przykłady

Przykład 1. Przyjmijmy, że tworzysz przyrostowe kopie zapasowe dwa razy dziennie (o północy i w południe) przez dwa dni, rozpoczynając od 31 stycznia 2011 r. Jeśli nazwa archiwum ma postać **MojeArchiwum-[DATE]**-, lista plików kopii zapasowych po zakończeniu drugiego dnia będzie następująca:

MojeArchiwum-1.31.2011-.tib (pełna, utworzona 31 stycznia o północy)
MojeArchiwum-1.31.2011-2.tib (przyrostowa, utworzona 31 stycznia w południe)
MojeArchiwum-2.1.2011-.tib (pełna, utworzona 1 lutego o północy)
MojeArchiwum-2.1.2011-2.tib (przyrostowa, utworzona 1 lutego w południe)

Przykład 2. Przyjmijmy, że tworzysz pełne kopie zapasowe według tego samego schematu, oraz używając takiej samej nazwy archiwum, jak w poprzednim przykładzie. Lista plików kopii zapasowych po zakończeniu drugiego dnia będzie wówczas następująca:

MojeArchiwum-1.31.2011-.tib (pełna, utworzona 31 stycznia w południe)
MojeArchiwum-2.1.2011-.tib (pełna, utworzona 1 lutego w południe)

Wynika to z zastąpienia pełnych kopii zapasowych utworzonych o północy przez nowe pełne kopie zapasowe utworzone w południe.

4.3.3 Podział kopii zapasowych i uproszczone nazewnictwo plików

Podczas podziału kopii zapasowej (s. 109) zgodnie z ustawieniami takie samo indeksowanie służy do nadawania nazw poszczególnym częściom kopii zapasowej. Do nazwy pliku kolejnej kopii zapasowej program przydzieli kolejny wolny indeks.

Przyjmijmy na przykład, że pierwsza kopia zapasowa archiwum **MojeDane** została podzielona na dwie części. Nazwy plików tej kopii zapasowej będą następujące: **MojeDane1.tib** i **MojeDane2.tib**. Kolejna kopia zapasowa (przyjmijmy, że nie jest dzielona) będzie miała nazwę **MojeDane3.tib**.

4.4 Tworzenie harmonogramu

Funkcja harmonogramu dostępna w oprogramowaniu Acronis umożliwia administratorowi dostosowanie planów tworzenia kopii zapasowych do codziennego cyklu funkcjonowania firmy i stylu

pracy każdego pracownika. Zadania planu są wykonywane systematycznie, a krytyczne dane skutecznie chronione.

Harmonogram jest dostępny podczas tworzenia planu tworzenia kopii zapasowych (s. 48) według jednego z następujących schematów tworzenia kopii zapasowych: Prosty, Niestandardowy lub Wieża Hanoi. Harmonogram można także ustawić dla zadań sprawdzania poprawności (s. 231).

Funkcja harmonogramu wykorzystuje lokalny czas komputera, na którym znajduje się plan tworzenia kopii zapasowych. Przed utworzeniem harmonogramu należy się upewnić, że ustawienia daty i godziny komputera są poprawne.

Harmonogram

Aby zdefiniować czas wykonywania zadania, należy określić jedno lub więcej zdarzeń. Zadanie zostanie uruchomione bezpośrednio po wystąpieniu jednego ze zdarzeń. W poniższej tabeli znajduje się lista zdarzeń dostępnych w systemach operacyjnych Windows i Linux.

Zdarzenie	Windows	Linux
Czas: Codziennie, Co tydzień, Co miesiąc	+	+
Czas, jaki upłynął od ostatniego pomyślnego utworzenia kopii zapasowej (można określić czas)	+	+
Logowanie użytkownika (dowolny użytkownik, bieżący użytkownik, określone konto użytkownika)	+	-
Wylogowanie użytkownika* (dowolny użytkownik, bieżący użytkownik, określone konto użytkownika) *Zamknięcie systemu nie jest tożsame z wylogowaniem użytkownika. Zadanie nie zostanie uruchomione przy zamknięciu systemu.	+	-
Uruchamianie systemu	+	+
Zmiana ilości wolnego miejsca (można określić wielkość zmiany ilości wolnego miejsca na dowolnym woluminie wybranym do tworzenia kopii zapasowej lub zawierającym dane przeznaczone do kopii zapasowej)	+	-
Zdarzenie w dzienniku zdarzeń systemu Windows (można określić parametry zdarzenia)	+	-
W przypadku alertu programu Acronis Drive Monitor	+	-

Warunek

W przypadku operacji tworzenia kopii zapasowych (i tylko takich operacji) oprócz zdarzeń można określić jeden lub więcej warunków. Po wystąpieniu dowolnego ze zdarzeń funkcja harmonogramu sprawdza warunek i w przypadku jego spełnienia uruchamia zadanie. W przypadku wielu warunków wszystkie z nich muszą być spełnione jednocześnie, aby program uruchomił zadanie. W poniższej tabeli znajduje się lista warunków dostępnych w systemach operacyjnych Windows i Linux.

Warunek: uruchom zadanie tylko jeśli...	Windows	Linux
Użytkownik jest bezczynny (uruchomiony jest wygaszacz ekranu lub komputer jest zablokowany)	+	-
Host lokalizacji jest dostępny	+	+
Czas wykonania zadania mieści się w określonym przedziale czasowym	+	+

Wszyscy użytkownicy są wylogowani	+	-
Minął określony czas od ostatniego pomyślnego utworzenia kopii zapasowej	+	+

Gdy wystąpi zdarzenie, a warunek (lub jeden z wielu warunków) nie zostanie spełniony, działanie funkcji harmonogramu określa opcja tworzenia kopii zapasowych Warunki uruchomienia zadania (s. 126).

Co się wydarzy, jeśli...

- **Co się wydarzy, jeśli zdarzenie wystąpi (a ewentualny warunek zostanie spełniony) w momencie, gdy wykonywanie poprzedniego zadania nie zostało zakończone?**
Zdarzenie zostanie zignorowane.
- **Co się wydarzy, jeśli zdarzenie wystąpi w momencie, gdy funkcja harmonogramu oczekuje na spełnienie warunku wymaganego przez poprzednie zdarzenie?**
Zdarzenie zostanie zignorowane.
- **Co się wydarzy, jeśli warunek pozostanie niespełniony przez bardzo długi czas?**
Jeżeli opóźnienie tworzenia kopii zapasowej staje się ryzykowne, można wymusić dany warunek (nakazać użytkownikom wylogowanie) lub uruchomić zadanie ręcznie. Aby zapewnić automatyczne postępowanie w takiej sytuacji, można ustawić czas, po upływie którego zadanie zostanie uruchomione niezależnie od spełnienia warunku.

4.4.1 Harmonogram dzienny

Harmonogram dzienny jest dostępny w systemach operacyjnych Windows i Linux.

Aby określić harmonogram dzienny

W obszarze **Harmonogram** zaznacz właściwy parametr w następujący sposób:

Co: <...> dzień/dni	Wyznacz częstotliwość wykonywania zadania. Jeżeli na przykład wybierzesz co 2 dni, zadanie będzie uruchamiane co drugi dzień.
----------------------------------	---

W obszarze **Wykonaj zadanie w ciągu dnia** zaznacz jedną z następujących opcji:

Raz o: <...>	Wyznacz godzinę jednokrotnego wykonania zadania.
Co: <...> Od: <...> do: <...>	Wyznacz, ile razy zadanie będzie wykonywane w określonym przedziale czasowym. Wyznaczenie częstotliwości zadania np. co godzinę od 10:00:00 do 22:00:00 umożliwia wykonanie zadania 12 razy jednego dnia: od 10 rano do 10 wieczorem.

W obszarze **Obowiązuje** określ następujące ustawienia:

Od: <...>	Wyznacz początkową datę obowiązywania harmonogramu (data rozpoczęcia obowiązywania). Jeżeli to pole wyboru nie jest zaznaczone, zadanie zostanie uruchomione najbliższego dnia o godzinie określonej powyżej.
Do: <...>	Wyznacz końcową datę obowiązywania harmonogramu. Jeżeli to pole wyboru nie jest zaznaczone, zadanie będzie uruchamiane przez nieskończoną liczbę dni.

Ustawienia zaawansowane harmonogramu (s. 85) są dostępne tylko w komputerach zarejestrowanych na serwerze Acronis Backup & Recovery 11 Management Server. Aby określić te ustawienia, kliknij **Zmień** w obszarze **Ustawienia zaawansowane**.

Wszystkie wybrane ustawienia są wyświetlane w polu **Wynik** na dole okna.

Przykłady

„Prosty” harmonogram dzienny

Uruchom zadanie codziennie o 18.00.

Parametry harmonogramu są następujące:

1. Co: **1** dzień.
2. Raz o: **18:00:00**.
3. Obowiązuje:
Od: **nie ustawiono**. Zadanie zostanie uruchomione w bieżącym dniu, jeżeli zostało utworzone przed 18.00. Zadanie utworzone po 18.00 zostanie uruchomione po raz pierwszy następnego dnia o tej porze.
Do: **nie ustawiono**. Zadanie będzie wykonywane przez nieskończoną liczbę dni.

Harmonogram „Trzygodzinny interwał czasu przez trzy miesiące”

Uruchom zadanie co trzy godziny. Zadanie rozpoczyna się w danym dniu (np. 15 września 2009 r.) i kończy po trzech miesiącach.

Parametry harmonogramu są następujące:

1. Co: **1** dzień.
2. Co: **3** godziny.
Od: **12:00:00** (północ) Do: **21:00:00** — tak więc zadanie zostanie wykonane 8 razy dziennie z 3 godzinną przerwą. Po ostatnim dziennym powtórzeniu o 21.00, nadchodzi następny dzień i zadanie rozpoczyna się ponownie od północy.
3. Obowiązuje:
Od: **15 września 2009**. Jeżeli zadanie zostało utworzone 15 września 2009 r. o 13.15, jego wykonanie rozpocznie się po nadejściu najwcześniejszego interwału czasowego: w naszym przykładzie o 15.00.
Do: **15 grudnia 2009**. W tym dniu zadanie zostanie wykonane po raz ostatni, ale będzie ono nadal dostępne w widoku **Zadania**.

Kilka harmonogramów dziennych dla jednego zadania

Są sytuacje, kiedy zadanie trzeba uruchomić kilka razy dziennie, a nawet kilka razy dziennie z różnymi interwałami czasowymi. W takich przypadkach można rozważyć przypisanie kilku harmonogramów do jednego zadania.

Załóżmy na przykład, że zadanie trzeba wykonać co trzeci dzień, zaczynając od 20 września 2009 r., pięć razy dziennie:

- pierwszy raz o 8.00,
- drugi raz o 12.00 (południe),
- trzeci raz o 15.00,
- czwarty raz o 17.00,
- piąty raz o 19.00.

Najbardziej oczywistym rozwiązaniem jest dodanie pięciu prostych harmonogramów. Po nieco dłuższym zastanowieniu można znaleźć bardziej optymalną metodę. Jak widać, interwał czasowy pomiędzy pierwszym a drugim wykonaniem zadania wynosi 4 godziny, a pomiędzy trzecim, czwartym

i piątym 2 godziny. W takim przypadku optymalne będzie przypisanie dwóch harmonogramów do zadania.

Pierwszy harmonogram dzienny

1. Co: **3** dni.
2. Co: **4** godziny.
Od: **08:00:00** Do: **12:00:00**.
3. Obowiązuje:
Od: **20 września 2009**.
Do: **nie ustawiono**.

Drugi harmonogram dzienny

1. Co: **3** dni.
2. Co: **2** godziny.
Od: **15:00:00** Do: **19:00:00**.
3. Obowiązuje:
Od: **20 września 2009**.
Do: **nie ustawiono**.

4.4.2 Harmonogram tygodniowy

Harmonogram tygodniowy jest dostępny w systemach operacyjnych Windows i Linux.

Aby określić harmonogram tygodniowy

W obszarze **Harmonogram** zaznacz właściwy parametr w następujący sposób:

Co: <...> tygodni w dniu: <...>	Określ liczbę tygodni oraz poszczególne dni tygodnia, kiedy zadanie będzie uruchamiane. Przy ustawieniu np. co 2 tygodnie w Pon zadanie będzie wykonywane co drugi tydzień w poniedziałek.
--	--

W obszarze **Wykonaj zadanie w ciągu dnia** zaznacz jedną z następujących opcji:

Raz o: <...>	Wyznacz godzinę jednokrotnego wykonania zadania.
Co: <...> Od: <...> do: <...>	Wyznacz, ile razy zadanie będzie wykonywane w określonym przedziale czasowym. Wyznaczenie częstotliwości zadania na przykład na co 1 godzinę od 10:00:00 do 22:00:00 umożliwia wykonanie zadania 12 razy jednego dnia: od 10 rano do 10 wieczorem.

W obszarze **Obowiązuje** określ następujące ustawienia:

Od: <...>	Wyznacz początkową datę obowiązywania harmonogramu (data rozpoczęcia obowiązywania). Jeżeli to pole wyboru nie jest zaznaczone, zadanie zostanie uruchomione najbliższego dnia o godzinie określonej powyżej.
Do: <...>	Wyznacz końcową datę obowiązywania harmonogramu. Jeżeli to pole wyboru nie jest zaznaczone, zadanie będzie uruchamiane przez nieskończoną liczbę tygodni.

Ustawienia zaawansowane harmonogramu (s. 85) są dostępne tylko w komputerach zarejestrowanych na serwerze Acronis Backup & Recovery 11 Management Server. Aby określić te ustawienia, kliknij **Zmień** w obszarze **Ustawienia zaawansowane**.

Wszystkie wybrane ustawienia są wyświetlane w polu **Wynik** na dole okna.

Przykłady

Harmonogram „Jeden dzień w tygodniu”

Uruchom zadanie w każdy piątek o 22.00 od określonego dnia (np. 14 maja 2009 r.) przez sześć miesięcy.

Parametry harmonogramu są następujące:

1. Co: **1** tydzień w: **Pią**.
2. Raz o: **22:00:00**.
3. Obowiązuje:

Od: **13 maja 2009**. Zadanie zostanie uruchomione w najbliższy piątek o 22.00.

Do: **13 listopada 2009**. W tym dniu zadanie zostanie wykonane po raz ostatni, ale po tej dacie będzie nadal dostępne w widoku Zadania (gdy data nie wypada w piątek, zadanie zostanie wykonane po raz ostatni w ostatni piątek poprzedzający tę datę).

Ten harmonogram jest powszechnie wykorzystywany przy niestandardowym schemacie tworzenia kopii zapasowych. Harmonogram typu „Jeden dzień w tygodniu” przypisuje się do pełnych kopii zapasowych, podczas gdy przyrostowe kopie bezpieczeństwa są zaplanowane w dni robocze. Szczegółowe informacje można znaleźć w przykładzie „Pełne i przyrostowe kopie zapasowe plus czyszczenie” w sekcji Schemat niestandardowy tworzenia kopii zapasowych (s. 59).

Harmonogram „W dni robocze”

Uruchom zadanie w każdym tygodniu w dni robocze: od poniedziałku do piątku. W dniu roboczym zadanie jest uruchamiane tylko raz o 21.00.

Parametry harmonogramu są następujące:

1. Co: **1** tydzień w: **<Dni robocze>** — po zaznaczeniu pola wyboru **<Dni robocze>** następuje automatyczne zaznaczenie odpowiednich pól (**Pon**, **Wto**, **Śro**, **Czw** i **Pią**), podczas gdy inne pola pozostają bez zmian.
2. Raz o: **21:00:00**.
3. Obowiązuje:

Od: **puste**. Po utworzeniu zadania — np. w poniedziałek o 11.30 — zostanie ono uruchomione tego samego dnia o 21.00. Gdy zadanie utworzymy np. w piątek po 21.00, wówczas zostanie ono uruchomione po raz pierwszy w najbliższym dniu roboczym (w naszym przykładzie w poniedziałek) o 21.00.

Data końcowa: **puste**. Zadanie będzie wykonywane przez nieskończoną liczbę tygodni.

Ten harmonogram jest powszechnie wykorzystywany przy niestandardowym schemacie tworzenia kopii zapasowych. Harmonogram typu „W dni robocze” przypisuje się do przyrostowych kopii zapasowych, podczas gdy wykonywanie pełnej kopii zapasowej jest zaplanowane raz w tygodniu. Szczegółowe informacje można znaleźć w przykładzie „Pełne i przyrostowe kopie zapasowe plus czyszczenie” w sekcji Schemat niestandardowy tworzenia kopii zapasowych (s. 59).

Kilka harmonogramów tygodniowych dla jednego zadania

Jeżeli trzeba wykonać zadanie w różne dni tygodnia z różnymi interwałami czasowymi, rozważ przypisanie specjalnego harmonogramu do każdego pożądanego dnia tygodnia lub do kilku dni.

Jeżeli na przykład zadanie ma być uruchamiane zgodnie z następującym harmonogramem:

- Poniedziałek: dwa razy — o 12.00 (południe) i 21.00

- Wtorek: co trzy godziny od 9.00 do 21.00
- Środa: co trzy godziny od 9.00 do 21.00
- Czwartek: co trzy godziny od 9.00 do 21.00
- Piątek: dwa razy — o 12.00 (południe) i 21.00 (tak samo jak w poniedziałek)
- Sobota: raz o 21.00
- Niedziela: raz o 21.00

Po połączeniu identycznych pór trzy następujące harmonogramy można przypisać do zadania:

Pierwszy harmonogram

1. Co: **1** tydzień w: **Pon, Pią.**
2. Co: **9** godzin.
Od: **12:00:00** Do: **21:00:00.**
3. Obowiązuje:
Od: **nie ustawiono.**
Do: **nie ustawiono.**

Drugi harmonogram

1. Co **1** tydzień w: **Wto, Śro, Czw.**
2. Co: **3** godziny.
Od: **09:00:00** do: **21:00:00.**
3. Obowiązuje:
Od: **nie ustawiono.**
Do: **nie ustawiono.**

Harmonogram trzeci

1. Co: **1** tydzień w: **Sob, Nie.**
2. Raz o: **21:00:00.**
3. Obowiązuje:
Od: **nie ustawiono.**
Do: **nie ustawiono.**

4.4.3 Harmonogram miesięczny

Harmonogram miesięczny jest dostępny w systemach operacyjnych Windows i Linux.

Aby określić harmonogram miesięczny

W obszarze **Harmonogram** zaznacz właściwy parametr w następujący sposób:

Miesiące: <...>	Wybierz miesiąc lub miesiące, kiedy zadanie ma być wykonywane.
Dni: <...>	Wybierz konkretne dni miesiąca, kiedy zadanie będzie wykonywane. Możesz również wybrać ostatni dzień miesiąca — niezależnie od jego faktycznej daty.
W: <...>	Wybierz konkretne dni tygodnia, kiedy zadanie ma być wykonywane.

W obszarze **Wykonaj zadanie w ciągu dnia** zaznacz jedno z następujących:

Raz o: <...>	Wyznacz godzinę jednokrotnego wykonania zadania.
---------------------	--

Co: <...>	Wyznacz, ile razy zadanie będzie wykonywane w określonym przedziale czasowym. Wyznaczenie częstotliwości zadania na przykład na co 1 godzinę od 10:00:00 do 22:00:00 umożliwia wykonanie zadania 12 razy jednego dnia: od 10 rano do 10 wieczorem.
Od: <...> do: <...>	

W obszarze **Obowiązuje** określ następujące ustawienia:

Od: <...>	Wyznacz początkową datę obowiązywania harmonogramu (data rozpoczęcia obowiązywania). Jeżeli to pole wyboru nie jest zaznaczone, zadanie zostanie uruchomione najbliższego dnia o godzinie określonej powyżej.
Do: <...>	Wyznacz końcową datę obowiązywania harmonogramu. Jeżeli to pole wyboru nie jest zaznaczone, zadanie będzie uruchamiane przez nieskończoną liczbę miesięcy.

Ustawienia zaawansowane harmonogramu (s. 85) są dostępne tylko w komputerach zarejestrowanych na serwerze Acronis Backup & Recovery 11 Management Server. Aby określić te ustawienia, kliknij **Zmień** w obszarze **Ustawienia zaawansowane**.

Wszystkie wybrane ustawienia są wyświetlane w polu **Wynik** na dole okna.

Przykłady

Harmonogram „Ostatni dzień każdego miesiąca”

Uruchom zadanie raz o 22.00 w ostatnim dniu każdego miesiąca.

Parametry harmonogramu są następujące:

1. Miesiące: **<Wszystkie miesiące>**.
2. Dni: **Ostatni**. Zadanie będzie wykonywane w ostatnim dniu każdego miesiąca — niezależnie od faktycznej daty.
3. Raz o: **22:00:00**.
4. Obowiązuje:
Od: **puste**.
Do: **puste**.

Ten harmonogram jest powszechnie wykorzystywany przy niestandardowym schemacie tworzenia kopii zapasowych. Harmonogram typu „Ostatni dzień miesiąca” przypisuje się do pełnych kopii zapasowych, podczas gdy wykonywanie różnicowych kopii bezpieczeństwa jest zaplanowane jeden raz w tygodniu, a przyrostowych — w dni robocze. Szczegółowe informacje można znaleźć w przykładzie „Pełne miesięczne, tygodniowe różnicowe i dzienne przyrostowe kopie zapasowe plus czyszczenie” w sekcji Schemat niestandardowy tworzenia kopii zapasowych (s. 59).

Harmonogram „Pora roku”

Uruchom zadanie we wszystkie dni jesieni na półkuli północnej w roku 2009 i 2010. W dniu roboczym zadanie będzie wykonywane co 6 godzin od 24.00 do 18.00.

Parametry harmonogramu są następujące:

1. Miesiące: **wrzesień, październik, listopad**.
2. W: **<wszystkie> <dni robocze>**.
3. Co: **6** godzin.
Od: **24:00:00** Do: **18:00:00**.
4. Obowiązuje:

Od: **30 sierpnia 2009**. Zadanie faktycznie zostanie uruchomione w pierwszym dniu września. Określając tę datę, po prostu ustalamy, że zadanie musi być uruchomione w 2009 roku.

Do: **1 grudnia 2010**. Zadanie faktycznie zakończy się w ostatnim dniu roboczym listopada. Określając tę datę, po prostu ustalamy, że zadanie musi zakończyć się w 2010 roku — po upływie jesieni na półkuli północnej.

Kilka harmonogramów miesięcznych dla jednego zadania

Jeżeli zadanie trzeba wykonać w różne dni lub w różne tygodnie z różnymi interwałami czasowymi w zależności od miesiąca, rozważ przypisanie specjalnego harmonogramu do każdego pożądanego miesiąca lub do kilku miesięcy.

Załóżmy, że zadanie zacznie obowiązywać od 1 listopada 2009 r.

- Podczas zimy na półkuli północnej zadanie jest uruchamiane jeden raz o 22.00 w każdy dzień roboczy.
- Podczas wiosny i jesieni na półkuli północnej zadanie jest uruchamiane co 12 godzin we wszystkie dni robocze.
- Podczas lata na półkuli północnej zadanie jest uruchamiane w każdy pierwszy i piętnasty dzień każdego miesiąca o 22.00.

W ten sposób do zadania przypisane zostały trzy następujące harmonogramy:

Pierwszy harmonogram

1. Miesiące: **grudzień, styczeń, luty**.
2. W: **<Wszystkie> <Dni robocze>**.
3. Raz o: **22:00:00**.
4. Obowiązuje:
Od: **1 listopada 2009**.
Do: **nie ustawiono**.

Drugi harmonogram

1. Miesiące: **marzec, kwiecień, maj, wrzesień, październik, listopad**.
2. W: **<Wszystkie> <Dni robocze>**.
3. Co: **12 godzin**
Od: **24:00:00** Do: **12:00:00**.
4. Obowiązuje:
Od: **1 listopada 2009**.
Do: **nie ustawiono**.

Harmonogram trzeci

1. Miesiące: **czerwiec, lipiec, sierpień**.
2. Dni: **1, 15**.
3. Raz o: **22:00:00**.
4. Obowiązuje:
Od: **1 listopada 2009**.
Do: **nie ustawiono**.

4.4.4 Po zdarzeniu zarejestrowanym w dzienniku systemu Windows

Ten typ harmonogramu ma zastosowanie tylko w systemach operacyjnych Windows.

Można zaplanować zadanie tworzenia kopii zapasowej po zarejestrowaniu danego zdarzenia w systemie Windows w jednym z dzienników zdarzeń, takim jak dziennik aplikacji, bezpieczeństwa lub systemowy.

Można na przykład skonfigurować plan tworzenia kopii zapasowych, który zapewni automatyczne wykonanie pełnej awaryjnej kopii zapasowej danych, kiedy tylko system Windows wykryje zbliżającą się awarię dysku twardego.

Parametry

Nazwa dziennika

Określa nazwę dziennika. Wybierz nazwę dziennika standardowego (**Aplikacja**, **Bezpieczeństwo** lub **System**) z listy lub wpisz nazwę dziennika — na przykład: **Microsoft Office Sessions**

Źródło zdarzenia

Określa źródło zdarzenia, zwykle wskazując komponent programu lub systemu, który spowodował zdarzenie — na przykład: **dysk**

Typ zdarzenia

Określa typ zdarzenia: **Błąd**, **Ostrzeżenie**, **Informacja**, **Powodzenie inspekcji** lub **Niepowodzenie inspekcji**.

Identyfikator zdarzenia

Określa numer zdarzenia, który zwykle umożliwia identyfikację konkretnego rodzaju zdarzeń wśród zdarzeń o takim samym źródle.

Na przykład zdarzenie **Błąd** o źródle **dysk** i identyfikatorze **7** występuje po wykryciu przez system Windows uszkodzonego sektora na dysku, natomiast zdarzenie **Błąd** o źródle **dysk** i identyfikatorze **15** występuje, kiedy dysk nie jest jeszcze gotowy do użycia.

Przykłady

Awaryjna kopia zapasowa po wykryciu „uszkodzonych sektorów”

Jeżeli na dysku twardym nagle pojawi się jeden lub więcej uszkodzonych sektorów, oznacza to, że wkrótce nastąpi awaria dysku twardego. Załóżmy, że chcesz utworzyć plan kopii zapasowych, który spowoduje skopiowanie danych z dysku twardego, gdy tylko wystąpi takie niebezpieczeństwo.

Kiedy system Windows wykryje uszkodzony sektor na dysku twardym, rejestruje zdarzenie o źródle **dysk** i identyfikatorze **7** w dzienniku **System**. Typ tego zdarzenia to **Błąd**.

Tworząc plan, wpisz lub wybierz następujące parametry w obszarze **Harmonogram**:

- **Nazwa dziennika:** **System**
- **Źródło zdarzenia:** **dysk**
- **Typ zdarzenia:** **Błąd**
- **Identyfikator zdarzenia:** **7**

Ważne: Aby zapewnić wykonanie tego zadania pomimo obecności sektorów uszkodzonych, trzeba wybrać ignorowanie takich sektorów w tym zadaniu. Aby to zrobić w **Opcje tworzenia kopii zapasowej**, przejdź do **Obsługa błędów**, a następnie zaznacz pole wyboru **Ignoruj sektory uszkodzone**.

Kopia zapasowa przed aktualizacją w systemie Vista

Założymy, że chcesz utworzyć plan tworzenia kopii zapasowych, który zapewni automatyczne wykonanie kopii zapasowej systemu — na przykład woluminu, na którym zainstalowany jest system Windows — przed instalacją każdej aktualizacji w systemie Windows.

Po pobraniu jednej lub więcej aktualizacji i zaplanowaniu ich instalacji, system operacyjny Microsoft Windows Vista rejestruje zdarzenie o źródle **Microsoft-Windows-WindowsUpdateClient** i identyfikatorze **18** w dzienniku **System**. Typ tego zdarzenia to **Informacja**.

Tworząc plan, wpisz lub wybierz następujące parametry w obszarze **Harmonogram**:

- **Nazwa dziennika:** System
- **Źródło zdarzenia:** Microsoft-Windows-WindowsUpdateClient
- **Typ zdarzenia:** Informacja
- **Identyfikator zdarzenia:** 18

Wskazówka: Aby skonfigurować podobny plan tworzenia kopii zapasowych dla komputerów z systemem Microsoft Windows XP, zastąp tekst w **Źródło zdarzenia** na **Agent aktualizacji Windows** i pozostaw niezmiennie inne pola.

Jak wyświetlić zdarzenia w Podglądzie zdarzeń

Otwieranie dziennika w Podglądzie zdarzeń

1. Na pulpicie lub w menu **Start** kliknij prawym przyciskiem myszy **Mój komputer**, a następnie **Zarządzaj**.
2. W konsoli **Zarządzanie komputerem**, rozwiń **Narzędzia systemowe**, a następnie **Podgląd zdarzeń**.
3. W pozycji **Podgląd zdarzeń** kliknij nazwę dziennika, który chcesz zobaczyć — na przykład **Aplikacja**.

Uwaga: Aby otworzyć dziennik bezpieczeństwa (**Bezpieczeństwo**), musisz być członkiem grupy administratorów.

Wyświetlanie właściwości zdarzenia, w tym źródła i numeru zdarzenia

1. W pozycji **Podgląd zdarzeń** kliknij nazwę dziennika, który chcesz zobaczyć — na przykład **Aplikacja**.

Uwaga: Aby otworzyć dziennik bezpieczeństwa (**Bezpieczeństwo**), musisz być członkiem grupy administratorów.

2. W liście zdarzeń w prawym panelu kliknij dwukrotnie nazwę zdarzenia, którego właściwości chcesz wyświetlić.
3. W oknie dialogowym **Właściwości zdarzenia** możesz wyświetlić właściwości zdarzenia, takie jak źródło zdarzenia pokazane w polu **Źródło** oraz numer zdarzenia pokazany w polu **Identyfikator zdarzenia**.

Po skończeniu kliknij **OK**, aby zamknąć okno dialogowe **Właściwości zdarzenia**.

4.4.5 W przypadku alertu programu Acronis Drive Monitor

Ten harmonogram ma zastosowanie w systemach operacyjnych Windows, w których jest zainstalowany program Acronis® Drive Monitor™.

Program Acronis Drive Monitor tworzy raporty na temat kondycji dysku twardego, korzystając z wewnętrznego systemu monitorowania tego dysku (S.M.A.R.T.). Na podstawie alertów programu Acronis Drive Monitor możesz skonfigurować awaryjne kopie zapasowe danych w uzupełnieniu regularnych kopii zapasowych. Tworzenie awaryjnej kopii zapasowej rozpoczyna się, gdy dyskowi zawierającemu dane grozi uszkodzenie.

Tworzenie kopii zapasowej rozpoczyna się natychmiast po osiągnięciu przez kondycję dysku poziomu ostrzegawczego lub krytycznego. Wskaźniki kondycji poszczególnych dysków (jako wartości procentowe) możesz sprawdzić, otwierając program Acronis Drive Monitor.

Alerty dotyczące temperatury dysku nie powodują rozpoczęcia tworzenia kopii zapasowej.

Wskazówka: Jeśli plan tworzenia kopii zapasowych używa niestandardowego schematu tworzenia kopii zapasowych (s. 59), możesz skonfigurować tworzenie awaryjnej kopii zapasowej, dodając dodatkowy harmonogram do tego samego planu tworzenia kopii zapasowych. Jeśli jest używany inny schemat tworzenia kopii zapasowych, musisz utworzyć osobny plan tworzenia kopii zapasowych.

4.4.6 Zaawansowane ustawienia harmonogramu

Po skonfigurowaniu w scentralizowanym planie tworzenia kopii zapasowych harmonogramu dziennego, tygodniowego lub miesięcznego dostępne są poniższe ustawienia zaawansowane.

Użyj Wake-on-LAN:

Po włączeniu tego ustawienia serwer Acronis Backup & Recovery 11 Management Server użyje funkcji Wake-on-LAN, aby o godzinie zaplanowanego utworzenia kopii zapasowej, czyszczenia lub sprawdzania poprawności wznowić pracę wyłączonych komputerów zarejestrowanych. Jeśli zadania tworzenia kopii zapasowej na poszczególnych komputerach rozpoczynają się z opóźnieniem (zobacz następne ustawienie), serwer zarządzania wznowi pracę komputerów zgodnie z określonymi opóźnieniami.

Przed zastosowaniem tego ustawienia należy się upewnić, że funkcja Wake-on-LAN jest włączona na zarejestrowanych komputerach. Konfiguracje podstawowego systemu wyjścia/wejścia (BIOS), karty sieciowej i systemu operacyjnego muszą zezwalać na wznawianie pracy komputera ze stanu wyłączzonego, nazywanego również stanem zasilania S5 lub G2.

Rozłóż uruchomienie w przedziale czasu

Po włączeniu tego ustawienia zadanie tworzenia kopii zapasowej na poszczególnych zarejestrowanych komputerach rozpocznie się z określonym opóźnieniem w stosunku do godziny rozpoczęcia ustawionej w planie tworzenia kopii zapasowych. Dzięki temu następuje rozłożenie faktycznych godzin rozpoczęcia zadań w ramach pewnego przedziału czasowego.

Ustawienie to można zastosować podczas definiowania scentralizowanego planu tworzenia kopii zapasowych wielu komputerów w lokalizacji sieciowej, aby uniknąć nadmiernego przeciążenia sieci.

Wartości opóźnienia wynoszą od zera do określonego maksimum i są ustalane na podstawie wybranej metody rozkładu.

Wartość opóźnienia dla poszczególnych komputerów jest ustalana podczas wdrażania planu tworzenia kopii zapasowych na tych komputerach. Pozostaje ona niezmienna do chwili ewentualnej edycji planu i zmiany maksymalnej wartości opóźnienia.

Spełnienie ewentualnych warunków jest sprawdzane o faktycznej godzinie rozpoczęcia zadania na każdym z komputerów.

Poniższe przykłady przedstawiają zastosowanie tego ustawienia.

Przykład 1

Założmy, że na trzech komputerach jest wdrażany scentralizowany plan tworzenia kopii zapasowych według następującego harmonogramu:

Uruchom zadanie: **Codziennie**

Raz o: **9:00:00**

Rozłóż uruchomienie w przedziale czasu

Maksymalne opóźnienie: **1 godzina**

Metoda rozkładu: **Losowa**

Wówczas na każdym z komputerów zadanie może rozpocząć się o dowolnej godzinie między 9:00:00 a 9:59:59 — na przykład:

Pierwszy komputer: codziennie o 9:30:03

Drugi komputer: codziennie o 9:00:00

Trzeci komputer: codziennie o 9:59:59

Przykład 2

Założmy, że na trzech komputerach jest wdrażany scentralizowany plan tworzenia kopii zapasowych według następującego harmonogramu:

Uruchom zadanie: **Codziennie**

Co: **2 godziny** Od: **9:00:00** Do: **11:00:00**

Rozłóż uruchomienie w przedziale czasu

Maksymalne opóźnienie: **1 godzina**

Metoda rozkładu: **Losowa**

Wówczas pierwsze uruchomienie zadania na każdym z komputerów może nastąpić o dowolnej godzinie między 9:00:00 a 9:59:59. Przerwa między pierwszym a drugim uruchomieniem wynosi dokładnie dwie godziny — na przykład:

Pierwszy komputer: codziennie o 9:30:03 oraz 11:30:03

Drugi komputer: codziennie o 9:00:00 oraz 11:00:00

Trzeci komputer: codziennie o 9:59:59 oraz 11:59:59

Aby określić ustawienia zaawansowane

1. Połącz się z serwerem zarządzania lub z zarejestrowanym na nim komputerem, a następnie rozpocznij tworzenie planu tworzenia kopii zapasowych.
2. W sekcji **Sposób tworzenia kopii zapasowej** wybierz Prosty, Wieża Hanoi lub Schemat niestandardowy, a następnie kliknij **Harmonogram**, aby określić harmonogram schematu.
3. W sekcji **Uruchom zadanie** wybierz **Codziennie**, **Co tydzień** lub **Co miesiąc**.
4. W obszarze **Ustawienia zaawansowane** kliknij **Zmień**.
5. Aby włączyć funkcję Wake-on-LAN, zaznacz pole wyboru **Użyj Wake-on-LAN**.
6. Aby rozłożyć godziny rozpoczęcia scentralizowanych zadań tworzenia kopii zapasowych, zaznacz pole wyboru **Rozłóż uruchomienie w przedziale czasu**, a następnie określ maksymalną wartość opóźnienia oraz metodę rozkładu.

4.4.7 Warunki

Warunki zwiększają elastyczność harmonogramu, ponieważ zadania tworzenia kopii zapasowych mogą być wykonywane zgodnie z podanymi warunkami. Gdy wystąpi określone zdarzenie (lista dostępnych zdarzeń znajduje się w sekcji „Tworzenie harmonogramu (s. 74)”), funkcja harmonogramu sprawdza określony warunek i w przypadku jego spełnienia wykonuje zadanie.

Gdy wystąpi zdarzenie, a warunek (lub jeden z wielu warunków) nie zostanie spełniony, działanie funkcji harmonogramu określa opcja tworzenia kopii zapasowych **Warunki uruchomienia zadania** (s. 126). Umożliwia ona określenie ważności warunków w strategii tworzenia kopii zapasowych:

- Spełnienie warunków jest obowiązkowe — zadanie tworzenia kopii zapasowej zostaje wstrzymane do czasu spełnienia wszystkich warunków.
- Spełnienie warunków jest preferowane, ale zadanie tworzenia kopii zapasowej ma wyższy priorytet — zadanie zostaje wstrzymane na pewien czas. Jeśli po upływie tego czasu warunki nadal pozostaną niespełnione, zadanie mimo to zostanie uruchomione. Przy tym ustawieniu program automatycznie rozwiązuje sytuację, w której warunki pozostają zbyt długo niespełnione, a dalsze opóźnianie kopii zapasowej jest niepożądane.
- Znaczenie ma czas uruchomienia zadania kopii zapasowej — zadanie tworzenia kopii zapasowej jest pomijane, jeżeli w chwili jego zaplanowanego uruchomienia warunki nie są spełnione. Pominięcie zadania jest sensowne, gdy kopię zapasową trzeba utworzyć o ściśle określonej godzinie, szczególnie w przypadku stosunkowo częstego występowania zdarzeń.

Warunki są dostępne tylko w przypadku korzystania z niestandardowego schematu tworzenia kopii zapasowych (s. 59). Warunki dla pełnych, przyrostowych i różnicowych kopii zapasowych można ustawić osobno.

Dodawanie wielu warunków

Aby umożliwić wykonanie zadania, wymagane jest jednoczesne spełnienie wielu warunków.

Przykład:

Zadanie tworzenia kopii zapasowej należy uruchomić, gdy na komputerze zarządzanym ilość wolnego miejsca zmieni się o przynajmniej 1 GB, ale tylko wtedy, gdy wszyscy użytkownicy są wylogowani i gdy od ostatniego utworzenia kopii zapasowej upłynęło ponad 12 godzin.

Harmonogram, warunki i opcję tworzenia kopii zapasowej **Warunki uruchomienia zadania** należy skonfigurować w następujący sposób:

- Harmonogram: **Gdy zmieni się ilość wolnego miejsca**; wartość: Uruchom zadanie, gdy ilość wolnego miejsca zmieni się o co najmniej: **1 GB**.
- Warunek: **Użytkownik wylogowany**; wartość: Uruchom zadanie zgodnie z planem tylko w przypadku, gdy wszyscy użytkownicy są wylogowani.
- Warunek: **Czas od utworzenia ostatniej kopii zapasowej**; wartość: Czas od utworzenia ostatniej kopii zapasowej: **12 godzin**.
- Warunki uruchomienia zadania: **Poczekaj na spełnienie warunków**.

Jeżeli ilość wolnego miejsca zmieni się o więcej niż 1 GB, funkcja harmonogramu poczeka na spełnienie obu pozostałych warunków i wówczas nastąpi uruchomienie zadania tworzenia kopii zapasowej.

Użytkownik jest bezczynny

Dotyczy: Windows

„Użytkownik jest beczynny” oznacza, że na komputerze zarządzanym uruchomiony jest wygaszacz ekranu lub komputer jest zablokowany.

Przykład:

Uruchom zadanie tworzenia kopii zapasowych na komputerze zarządzanym codziennie o 21.00, najlepiej kiedy użytkownik jest beczynny. Jeśli użytkownik będzie nadal aktywny do godziny 23.00, uruchom zadanie pomimo wszystko.

- Zdarzenie: **Codziennie**, co 1 dzień/dni; Raz o: **21:00:00**.
- Warunek: **Użytkownik jest beczynny**.
- Warunki rozpoczęcia zadania: **Poczekaj na spełnienie warunków**. Uruchom zadanie po upływie 2 godzin(y).

Wskutek tego:

(1) Jeśli użytkownik przejdzie w stan beczynności przed 21.00, zadanie tworzenia kopii zapasowej rozpocznie się o 21.00.

(2) Jeśli użytkownik przejdzie w stan beczynności pomiędzy 21.00 a 23.00, zadanie tworzenia kopii zapasowej rozpocznie się natychmiast po wejściu w stan beczynności.

(3) Jeśli jeden z użytkowników będzie nadal zalogowany o 23.00, tworzenie kopii zapasowej rozpocznie się pomimo wszystko.

Lokalizacja jest dostępna

Dotyczy: Windows, Linux

„Lokalizacja jest dostępna” oznacza, że docelowe miejsce przechowywania archiwów na dysku sieciowym jest dostępne w celu utworzenia kopii zapasowej.

Przykład:

Tworzenie kopii zapasowej w lokalizacji sieciowej odbywa się w dni robocze o 21.00. Jeśli lokalizacja o tej porze jest niedostępna (np. z powodu prac konserwacyjnych), pomiń tworzenie kopii zapasowej i poczekaj do następnego dnia roboczego, aby rozpocząć zadanie. Zakłada się, że zadanie raczej nie powinno wcale się rozpocząć niż zakończyć niepomyślnie.

- Zdarzenie: **Co tydzień**, Co 1 tydzień/tyg. w <dni robocze>; Raz o **21:00:00**.
- Warunek: **Lokalizacja jest dostępna**
- Warunki uruchomienia zadania: **Pomiń wykonywanie zadania**.

Wskutek tego:

(1) Jeśli nadejdzie 21.00 i lokalizacja archiwum będzie dostępna, zadanie tworzenia kopii zapasowej rozpocznie się dokładnie o tej godzinie.

(2) Jeśli nadejdzie 21.00, a lokalizacja archiwum będzie niedostępna, zadanie tworzenia kopii zapasowej rozpocznie się w następnym dniu roboczym, w którym lokalizacja będzie dostępna.

(3) Jeśli lokalizacja nie będzie dostępna w żaden dzień roboczy o godzinie 21.00, zadanie nie rozpocznie się nigdy.

Mieści się w przedziale czasu

Dotyczy: Windows, Linux

Ogranicza porę rozpoczęcia tworzenia kopii zapasowej do określonego interwału czasowego.

Przykład

Firma używa pamięci masowej w różnych lokalizacjach tej samej sieci w celu tworzenia kopii zapasowych danych użytkowników i serwerów. Dzień roboczy rozpoczyna się o 8.00 i kończy o 17.00. Kopia bezpieczeństwa danych użytkowników jest tworzona natychmiast po wylogowaniu użytkowników, ale nie wcześniej niż o 16.30 i nie później niż o 22.00. Kopia zapasowa danych na serwerze jest tworzona codziennie o 23.00. Zatem najlepiej utworzyć kopię zapasową danych wszystkich użytkowników przed tą godziną, aby nie blokować przepustowości sieci. Określając górny limit na 22.00, zakłada się, że tworzenie kopii zapasowych danych użytkowników nie zajmie więcej niż godzinę. Jeżeli jakiś użytkownik nadal będzie zalogowany w określonym interwale czasowym lub wyloguje się o dowolnej innej porze — kopia zapasowa danych użytkowników nie jest tworzona, to znaczy wykonanie zadania zostaje pominięte.

- Zdarzenie: **Przy wylogowywaniu**, Następujący użytkownik: **Dowolny użytkownik**.
- Warunek: **Mieści się w przedziale czasu**, od **16:30:00** do **22:00:00**.
- Warunki uruchomienia zadania: **Pomiń wykonywanie zadania**.

Wskutek tego:

(1) jeśli użytkownik wyloguje się pomiędzy 16:30:00 a 22:00:00, tworzenie kopii zapasowej rozpocznie się natychmiast po wylogowaniu;

(2) jeśli użytkownik wyloguje się o dowolnej innej porze, wykonanie zadania zostanie pominięte.

Co jeśli...

Co jeśli według harmonogramu zadanie ma być wykonane o określonej porze, a pora ta nie mieści się w określonym interwale czasu?

Na przykład:

- Zdarzenie: **Codziennie**, Co **1** dzień; Raz o **15:00:00**.
- Warunek: **Mieści się w przedziale czasu**, od **18:00:00** do **23:59:59**.

W tym przykładzie to, czy i kiedy zadanie zostanie uruchomione, zależy od warunków uruchomienia zadania:

- Jeśli warunek uruchomienia zadania to **Pomiń wykonywanie zadania**, zadanie nie zostanie uruchomione nigdy.
- Jeśli warunek uruchomienia zadania to **Poczekaj na spełnienie warunków**, a pole wyboru **Uruchom zadanie po upływie** będzie *odznaczone*, zadanie (zaplanowane na 15.00) rozpocznie się o 18.00 — o godzinie, kiedy warunek zostanie spełniony.
- Jeśli warunek uruchomienia zadania to **Poczekaj na spełnienie warunków**, a pole wyboru **Uruchom zadanie po upływie** będzie *zaznaczone* z czasem oczekiwania powiedzmy **1 godzina**, zadanie (zaplanowane na 15.00) rozpocznie się o 16.00 — o godzinie, kiedy skończy się okres oczekiwania.

Użytkownik wylogowany

Dotyczy: Windows

Uruchomienie zadania tworzenia kopii zapasowej zostaje wstrzymane do czasu, kiedy wszyscy użytkownicy wylogują się z systemu Windows na komputerze zarządzanym.

Przykład

Uruchom zadanie tworzenia kopii zapasowej o 20.00 w pierwszy i trzeci piątek każdego miesiąca, najlepiej po wylogowaniu wszystkich użytkowników. Jeśli o 23.00 jeden z użytkowników będzie nadal zalogowany, uruchom zadanie pomimo wszystko.

- Zdarzenie: **Co miesiąc**, Miesiące: **<Wszystkie>**; W: **<Pierwszy>**, **<Trzeci>** **<Piątek>**; Raz o **20:00:00**.
- Warunek: **Użytkownik wylogowany**.
- Warunki rozpoczęcia zadania: **Poczekaj na spełnienie warunków**. Uruchom zadanie po upływie **3** godzin.

Wskutek tego:

- (1) jeśli wszyscy użytkownicy zostali wylogowani o 20.00, tworzenie kopii zapasowej rozpocznie się o 20.00;
- (2) jeśli ostatni użytkownik wyloguje się pomiędzy 20.00 a 23.00, tworzenie kopii zapasowej rozpocznie się natychmiast po wylogowaniu;
- (3) jeśli jeden z użytkowników będzie nadal zalogowany o 23.00, tworzenie kopii zapasowej rozpocznie się pomimo wszystko.

Czas od utworzenia ostatniej kopii zapasowej

Dotyczy systemu: Windows, Linux

Wykonywanie zadania tworzenia kopii zapasowej zostaje wstrzymane do momentu, aż od ostatniego pomyślnego utworzenia kopii zapasowej upłynie określony czas.

Przykład:

Zadanie tworzenia kopii zapasowej ma być uruchamiane przy uruchamianiu systemu, ale tylko wtedy, gdy od ostatniego pomyślnego utworzenia kopii zapasowej upłynęło ponad 12 godzin.

- Zdarzenie: **Przy uruchamianiu**; Rozpocznij zadanie po uruchomieniu komputera.
- Warunek: **Czas od utworzenia ostatniej kopii zapasowej**; Czas od utworzenia ostatniej kopii zapasowej: **12 godzin**.
- Warunki uruchomienia zadania: **Poczekaj na spełnienie warunków**.

Wskutek tego:

- (1) Jeśli komputer zostanie ponownie uruchomiony przed upływem 12 godzin od ostatniego pomyślnego utworzenia kopii zapasowej, funkcja harmonogramu zaczeka, aż upłynie 12 godzin, i dopiero wtedy uruchomi zadanie.
- (2) Jeśli komputer zostanie ponownie uruchomiony po upływie 12 godzin od ostatniego pomyślnego utworzenia kopii zapasowej, zadanie tworzenia kopii zapasowej rozpocznie się natychmiast.
- (3) Jeśli komputer nie zostanie nigdy ponownie uruchomiony, zadanie nigdy się nie rozpocznie. W razie potrzeby tworzenie kopii zapasowej można uruchomić ręcznie w widoku **Plany i zadania tworzenia kopii zapasowych**.

4.5 Replikacja i przechowywanie kopii zapasowych

W trakcie tworzenia planu tworzenia kopii zapasowych (s. 48) określ podstawową lokalizację kopii zapasowych. Ponadto możesz wykonać następujące czynności:

- Replikować (kopiować) każdą kopię zapasową do innej lokalizacji natychmiast po jej utworzeniu.
- Przechowywać kopie zapasowe zgodnie z określonymi regułami przechowywania, po czym przenosić je do drugiej lokalizacji lub usuwać je.

W podobny sposób można kopiować i przenosić kopie zapasowe z lokalizacji drugiej do trzeciej i tak dalej. Obsługiwanych jest do pięciu kolejnych lokalizacji (uwzględniając lokalizację podstawową).

Uwaga: Funkcja replikacji zastąpiła i rozszerzyła opcję **Dwa miejsca docelowe** dostępną w programie Acronis Backup & Recovery 10.

Przykład. Tworzysz kopię zapasową komputera w folderze lokalnym. Jest ona natychmiast kopiowana do folderu sieciowego. Kopia jest przechowywana w oryginalnym folderze lokalnym tylko przez miesiąc.

Opisany scenariusz przedstawia poniższa ilustracja.



Scenariusze użycia

- **Niezawodne odzyskiwanie po awarii** (s. 96)
Kopie zapasowe przechowuj zarówno lokalnie (w celu natychmiastowego odzyskania danych), jak i w innej lokalizacji (w celu zabezpieczenia kopii zapasowych przez awarię lokalnego magazynu lub klęską żywiołową).
- **Przechowywanie jedynie ostatnich punktów odzyskiwania** (s. 97)
Usuwać starsze kopie zapasowe z magazynu o szybkim dostępie zgodnie z regułami przechowywania, zapobiegając nadużywaniu kosztownego miejsca do przechowywania.
- **Niższe koszty przechowywania danych w kopiach zapasowych** (s. 97)
W okresie większego prawdopodobieństwa korzystania z kopii zapasowych przechowuj je w magazynie o szybkim dostępie. Następnie, w celu długookresowego składowania, przenieś je do tańszego magazynu. Takie postępowanie pozwala na spełnienie wymogów prawnych związanych z przechowywaniem danych.
- **Tworzenie kopii zapasowej na wolnym urządzeniu w wąskim oknie tworzenia kopii zapasowych** (s. 98)
Nocne kopie zapasowe twórz w skarbku zarządzanym znajdującym się w magazynie o szybkim dostępie, a następnie pozwól węzłowi Acronis Backup & Recovery 11 Storage Node na ich przeniesienie na taśmę w ciągu dnia.

Reguły replikacji i przechowywania w schematach tworzenia kopii zapasowych

Poniższa tabela przedstawia dostępność reguł replikacji i przechowywania w różnych schematach tworzenia kopii zapasowych.

Schemat tworzenia kopii zapasowych	Możliwość kopiowania kopii zapasowych	Możliwość przenoszenia kopii zapasowych	Możliwość usuwania kopii zapasowych
Uruchom teraz (s. 56)	Tak	Nie	Nie

Uruchamianie ręczne (s. 64)	Tak	Nie	Nie
Prosty (s. 55)	Tak	Tak	Tak
Dziadek-ojciec-syn (GFS) (s. 56)	Tak	Nie	Tak
Wieża Hanoi (s. 62)	Tak	Nie	Tak
Niestandardowy (s. 59)	Tak	Tak	Tak
Pierwotna kopia zapasowa w magazynie	Nie	Nie	Nie

Uwagi:

- Nie jest możliwe jednoczesne skonfigurowanie kopiowania i przenoszenia kopii zapasowych z tej samej lokalizacji.
- Uprozczone nazewnictwo plików kopii zapasowych (s. 70) nie pozwala na korzystanie z replikacji ani reguł przechowywania.

4.5.1 Obsługiwane lokalizacje

Kopię zapasową można kopiować lub przenosić z dowolnej z następujących lokalizacji:

- Folder lokalny na dysku stałym lub wymiennym
- Folder sieciowy
- Serwer FTP lub SFTP
- Acronis Backup & Recovery 11 Storage Node
- Strefa Acronis Secure Zone

Kopię zapasową można kopiować lub przenosić *do* dowolnej z następujących lokalizacji:

- Folder lokalny na dysku stałym lub wymiennym
- Folder sieciowy
- Serwer FTP lub SFTP
- Acronis Backup & Recovery 11 Storage Node
- Urządzenie taśmowe

Kopie zapasowe skopiowane lub przeniesione do innej lokalizacji nie są zależne od kopii zapasowych pozostałych w oryginalnej lokalizacji i na odwrót. Dane można odzyskać z dowolnej kopii zapasowej bez dostępu do pozostałych lokalizacji.

Ograniczenia

- Kopiowanie i przenoszenie kopii zapasowych *na i z* dysków optycznych (CD, DVD, Blu-ray) nie jest obsługiwane.
- Kopiowanie i przenoszenie kopii zapasowych z węzła magazynowania Acronis Backup & Recovery 11 Storage Node *do* folderu lokalnego nie jest obsługiwane.
- Urządzenie taśmowe może pełnić jedynie rolę lokalizacji docelowej. Dalsze kopiowanie ani przenoszenie kopii zapasowych z takiego urządzenia nie jest możliwe.
- Program nie umożliwia kilkukrotnego określenia tej samej lokalizacji. Nie można na przykład przenieść kopii zapasowej z jednego folderu do innego, a następnie z powrotem do folderu oryginalnego.

Na którym komputerze jest wykonywana operacja?

Kopiowanie, przenoszenie lub usuwanie kopii zapasowej z dowolnej lokalizacji rozpoczyna agent, który utworzył kopię zapasową. Operację tę wykonuje:

- ten agent, jeśli lokalizacją *nie jest* skarbiec zarządzany.
- odpowiedni węzeł magazynowania, jeśli lokalizacją *jest* skarbiec zarządzany.

Jak wynika z powyższego opisu, operacja ta zostanie przeprowadzona jedynie wtedy, gdy komputer z agentem jest włączony. Jeśli jest ona zaplanowana, w harmonogramie będzie obowiązywać data i godzina tego komputera.

4.5.2 Konfigurowanie replikacji kopii zapasowych

Replikację kopii zapasowych można skonfigurować w trakcie tworzenia planu tworzenia kopii zapasowych (s. 48).

- Aby skonfigurować replikację z lokalizacji podstawowej, zaznacz pole wyboru **Replikuj nowo utworzoną kopię zapasową do innej lokalizacji**.
- Aby skonfigurować replikację z drugiej lub każdej kolejnej lokalizacji, zaznacz pole wyboru **Replikuj kopie zapasowe do innej lokalizacji, gdy tylko pojawią się w tej lokalizacji**.

Następnie wybierz lokalizację replikacji kopii zapasowych. Gdy tylko kopia zapasowa pojawi się w poprzedniej lokalizacji, zostanie poddana replikacji do kolejnej.

Jeśli pozwala na to schemat tworzenia kopii zapasowych, możesz także określić czas automatycznego usuwania kopii zapasowych z każdej z tych lokalizacji.

4.5.3 Konfigurowanie reguł przechowywania kopii zapasowych

Reguły przechowywania kopii zapasowych można skonfigurować podczas tworzenia planu tworzenia kopii zapasowych (s. 48). Dostępne reguły przechowywania zależą od wybranego schematu tworzenia kopii zapasowych.

Stosowanie reguł przechowywania może być ograniczone opcją **Czas braku aktywności replikacji/czyszczenia** (s. 96).

Schemat prosty

Każda kopia zapasowa jest przechowywana do momentu przekroczenia określonego limitu czasu. Następnie zostaje usunięta lub przeniesiona.

Aby skonfigurować usuwanie kopii zapasowych:

- W **Regułach przechowywania** kliknij **Usuń kopie zapasowe starsze niż**, a następnie zdefiniuj okres przechowywania.

Aby skonfigurować przenoszenie kopii zapasowych:

- W **Regułach przechowywania** kliknij **Przeń kopie zapasowe starsze niż**, a następnie zdefiniuj okres przechowywania. W polu **Miejsce replikacji/przenoszenia kopii zapasowych** określ lokalizację.

Reguły przechowywania zostaną zastosowane po utworzeniu kopii zapasowej. Utworzenie kopii zapasowej w odniesieniu do drugiej i kolejnych lokalizacji oznacza skopiowanie lub przeniesienie kopii z poprzedniej lokalizacji.

Schemat Dziadek-ojciec-syn (GFS)

Kopie zapasowe każdego typu (dzienne, tygodniowe i miesięczne) są przechowywane przez okres zdefiniowany w polu **Zachowuj kopie zapasowe**, po czym zostają usunięte.

Reguły przechowywania zostaną zastosowane po utworzeniu kopii zapasowej. Są one stosowane kolejno w lokalizacji podstawowej, drugiej i każdej kolejnej.

Schemat Wieża Hanoi

Okres przechowywania każdej kopii zapasowej jest zależny od jej poziomu (s. 62). Po jego upływie kopia jest usuwana. Liczbę poziomów określa się w polu **Liczba poziomów**.

Reguły przechowywania zostaną zastosowane po utworzeniu kopii zapasowej. Są one stosowane kolejno w lokalizacji podstawowej, drugiej i każdej kolejnej.

Schemat niestandardowy

Każda z kopii zapasowych jest przechowywana do momentu spełnienia określonych reguł. Następnie zostaje usunięta lub przeniesiona.

Aby skonfigurować usuwanie kopii zapasowych:

- W polu **Czyszczenie archiwum** wybierz **Korzystanie z reguł przechowywania**. Określ reguły w oknie **Reguły przechowywania** (s. 94) i wybierz **Jeśli określone warunki zostały spełnione: Usuń najstarsze kopie zapasowe**.
- W polu **Zastosuj reguły przechowywania** określ czas zastosowania reguł.

Aby skonfigurować przenoszenie kopii zapasowych:

- W polu **Czyszczenie archiwum** wybierz **Korzystanie z reguł przechowywania**. Określ reguły w oknie **Reguły przechowywania** (s. 94) i wybierz **Jeśli określone warunki zostały spełnione: Przenieś najstarsze kopie zapasowe do innej lokalizacji**. Kliknij **OK**, a następnie określ lokalizację w polu **Miejsce replikacji/przenoszenia kopii zapasowych**.
- W polu **Zastosuj reguły przechowywania** określ czas zastosowania reguł.

Możesz wybrać opcję zastosowania reguł przechowywania przed utworzeniem kopii zapasowej, po jej utworzeniu, zgodnie z harmonogramem lub wskazać kombinację tych opcji. Utworzenie kopii zapasowej w odniesieniu do drugiej i kolejnych lokalizacji oznacza skopiowanie lub przeniesienie kopii z poprzedniej lokalizacji.

4.5.4 Reguły przechowywania schematu niestandardowego

W oknie **Reguły przechowywania** można wybrać okres przechowywania kopii zapasowych w lokalizacji oraz określić, czy przenieść je czy usunąć po jego upływie.

Reguły zostaną zastosowane wobec wszystkich kopii zapasowych wykonanych na *określonym komputerze* i umieszczonych w *określonej lokalizacji* przez *określony plan tworzenia kopii zapasowych*. Taki zestaw kopii zapasowych w programie Acronis Backup & Recovery 11 jest określany mianem *archiwum*.

Aby skonfigurować reguły przechowywania kopii zapasowych:

1. Określ jedną z następujących możliwości (opcje (a) i (b) wzajemnie się wykluczają):

- a. **Kopie zapasowe starsze niż...** i/lub **Rozmiar archiwum większy niż...**

Kopia zapasowa będzie przechowywana do czasu spełnienia określonego warunku (lub obu warunków).

Przykład:

Kopie zapasowe starsze niż 5 dni

Rozmiar archiwum większy niż 100 GB

W przypadku takich ustawień kopia zapasowa będzie przechowywana dopóty, dopóki nie będzie starsza niż pięć dni i rozmiar zawierającego ją archiwum nie przekroczy 100 GB.

b. Liczba kopii zapasowych w archiwum przekracza...

Jeśli liczba kopii zapasowych przekroczy określoną wartość, nastąpi przeniesienie lub usunięcie jednej lub większej liczby najstarszych kopii. Ustawienie minimalne wynosi 1.

2. Określ, czy po spełnieniu określonych warunków chcesz usunąć kopie zapasowe czy przenieść je do innej lokalizacji.

Po kliknięciu **OK** możesz określić, gdzie chcesz przenieść kopie zapasowe, i skonfigurować reguły przechowywania tej lokalizacji.

Usuwanie ostatniej kopii zapasowej w archiwum

Reguły przechowywania są stosowane, jeśli archiwum zawiera więcej niż jedną kopię zapasową. Oznacza to, że ostatnia kopia zapasowa w archiwum zostanie zachowana nawet wtedy, gdy naruszy to regułę przechowywania. Nie należy usuwać jedynej posiadanej kopii zapasowej, stosując reguły przechowywania *przed* utworzeniem kopii zapasowej. To nie zadziała. Jeśli akceptujesz ryzyko utraty ostatniej kopii zapasowej, użyj ustawienia alternatywnego **Czyszczenie archiwum > Gdy w trakcie tworzenia kopii zapasowej zabraknie miejsca** (s. 59).

Usuwanie lub przenoszenie kopii zapasowych z zależnościami

Aby uzyskać dostęp do tych ustawień, w oknie **Reguły przechowywania** kliknij **Pokaż ustawienia zaawansowane**.

Reguły przechowywania zakładają usuwanie lub przenoszenie niektórych kopii zapasowych i zachowywanie innych. Co jednak dzieje się w przypadku, gdy archiwum zawiera przyrostowe i różnicowe kopie zapasowe, które są zależne od siebie i od pełnych kopii zapasowych, na których są oparte? Nie można na przykład usunąć przestarzałej pełnej kopii zapasowej i zachować jej przyrostowych elementów podrzędnych.

Gdy usunięcie lub przeniesienie jednej kopii zapasowej wpływa na inne kopie zapasowe, stosowana jest jedna z następujących reguł:

- **Przechowuj kopię zapasową, dopóki nie zostaną usunięte (przeniesione) wszystkie zależne kopie zapasowe.**

Przestarzała kopia zapasowa będzie przechowywana, dopóki wszystkie zależne od niej kopie zapasowe także nie staną się przestarzałe. Następnie podczas regularnego czyszczenia zostanie usunięty cały łańcuch naraz. Jeśli zostanie wybrana opcja przenoszenia nieaktualnych kopii zapasowych do kolejnej lokalizacji, kopia zapasowa zostanie skopiowana bez żadnego opóźnienia. Jedynie jej usunięcie z aktualnej lokalizacji zostanie opóźnione.

Ten tryb pomaga uniknąć potencjalnej, czasochłonnej konsolidacji, ale wymaga dodatkowego miejsca na przechowywanie kopii zapasowych, których usunięcie zostało opóźnione. Rozmiar archiwum lub wiek bądź liczba kopii zapasowych może przekroczyć wartości określone przez użytkownika.

- **Konsoliduj te kopie zapasowe**

Program skonsoliduje kopię zapasową przeznaczoną do usunięcia lub przeniesienia z następną zależną od niej kopią zapasową. Na przykład reguły przechowywania wymagają usunięcia pełnej kopii zapasowej i zachowania następnej, przyrostowej. Kopie te zostaną scalone w jedną pełną kopię zapasową, która otrzyma datę utworzenia przyrostowej kopii zapasowej. Po usunięciu

przyrostowej lub różnicowej kopii zapasowej ze środka tańcucha wynikowa kopia zapasowa będzie kopią typu przyrostowego.

Ten tryb gwarantuje, że po każdym czyszczeniu rozmiar archiwum oraz wiek i liczba kopii zapasowych będą się mieścić w granicach określonych przez użytkownika. Jednak konsolidacja może pochłonąć mnóstwo czasu i zasobów systemowych. Poza tym w skarbcu będzie potrzebne dodatkowe miejsce na pliki tymczasowe tworzone podczas konsolidacji.

Co trzeba wiedzieć o konsolidacji

Należy pamiętać, że konsolidacja to jedynie metoda usuwania, ale nie alternatywa do 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.

4.5.5 Czas braku aktywności replikacji/czyszczenia

Ta opcja jest dostępna tylko w przypadku skonfigurowania reguł replikacji lub przechowywania (s. 90) kopii zapasowych.

Wskazuje ona okres, w którym nie można rozpocząć replikacji ani stosowania reguł przechowywania. Operacje te zostaną przeprowadzone po upływie czasu braku aktywności, jeśli komputer będzie wówczas włączony. Operacje uruchomione przed rozpoczęciem czasu braku aktywności będą kontynuowane bez przerywania.

Czas braku aktywności dotyczy wszystkich lokalizacji, w tym lokalizacji podstawowej.

Ustawienie wstępne: **Wyłączone**.

Aby określić czas braku aktywności, zaznacz pole wyboru **Nie rozpoczynaj replikacji/czyszczenia w następującym przedziale czasu**, a następnie wybierz dni oraz okres w ciągu dnia.

Przykład użycia

Warto użyć tej opcji do oddzielenia procesu tworzenia kopii zapasowej od zadań replikacji lub czyszczenia. Przyjmijmy, że tworzysz w trakcie dnia lokalne kopie zapasowe komputerów i replikujesz je do folderu sieciowego. Zdefiniuj czas braku aktywności tak, aby obejmował godziny pracy. Replikacja zostanie przeprowadzona po godzinach pracy, gdy obciążenie sieci jest niższe.

4.5.6 Przykłady użycia

W tej sekcji przedstawiono przykładowe możliwości replikowania kopii zapasowych i konfigurowania związanych z nimi reguł przechowywania.

Przykład 1. Replikacja kopii zapasowych do folderu sieciowego

Rozważmy następujący scenariusz:

- Chcesz codziennie ręcznie tworzyć pełną kopię zapasową swojego komputera.
- Chcesz zapisywać kopie zapasowe w strefie Acronis Secure Zone (s. 188) na komputerze.
- Chcesz przechowywać kopie kopii zapasowych w folderze sieciowym.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych w ramach schematu **Uruchamianie ręczne**. Podczas tworzenia planu tworzenia kopii zapasowych w polu **Ścieżka** określ Acronis Secure Zone, w polu **Typ kopii zapasowej** wybierz **Pełna**, zaznacz pole wyboru **Replikuj nowo utworzoną kopię zapasową do innej lokalizacji**, a następnie w polu **2. lokalizacja** określ folder sieciowy.

Wynik:

- Możesz odzyskać woluminy lub pliki komputera z łatwo dostępnej lokalnej kopii zapasowej przechowywanej w specjalnym obszarze dysku twardego.
- Jeśli dysk twardy ulegnie awarii, możesz odzyskać komputer z folderu sieciowego.

Przykład 2. Ograniczenie okresu przechowywania i całkowitego rozmiaru przechowywanych kopii zapasowych

Rozważmy następujący scenariusz:

- Chcesz co tydzień tworzyć pełną kopię zapasową swojego komputera.
- Chcesz przechowywać wszystkie kopie zapasowe młodsze niż miesiąc.
- Chcesz przechowywać nawet starsze kopie zapasowe, jeśli tylko ich całkowity rozmiar jest mniejszy niż 200 GB.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych w ramach schematu **Niestandardowy**. W trakcie tworzenia planu tworzenia kopii zapasowych określ tygodniowy harmonogram tworzenia pełnej kopii zapasowej. W polu **Czyszczenie archiwum** wybierz **Korzystanie z reguł przechowywania**.

Kliknij **Reguły przechowywania**, zaznacz pola wyboru **Kopie zapasowe starsze niż** oraz **Rozmiar archiwum większy niż**, a następnie wybierz odpowiednio **1 miesiąc** i **200 GB**. W polu **Jeśli określone warunki zostały spełnione** wybierz **Usuń najstarsze kopie zapasowe**.

Kliknij **OK**. W obszarze **Zastosuj reguły przechowywania** zaznacz pole wyboru **Po utworzeniu kopii zapasowej**.

Wynik:

- Kopie zapasowe będą przechowywane przez co najmniej miesiąc bez względu na ich całkowity rozmiar.
- Kopie zapasowe starsze niż miesiąc będą przechowywane pod warunkiem, że całkowity rozmiar wszystkich kopii zapasowych (starszych i młodszych) nie przekracza 200 GB. W innym razie program usunie niektóre lub wszystkie starsze kopie zapasowe, rozpoczynając od najstarszej.

Przykład 3. Przenoszenie starszych kopii zapasowych na taśmy

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć kopię zapasową swojego komputera.
- Chcesz przez tydzień przechowywać kopie zapasowe lokalnie.
- Chcesz przenosić kopie zapasowe starsze niż tydzień na urządzenie taśmowe.

Scenariusz taki określa się czasem mianem archiwizacji etapowej lub D2D2T (dysk-dysk-taśma).

W tym scenariuszu utwórz plan tworzenia kopii zapasowych w ramach schematu **Prosty**, zawierający codzienny harmonogram (domyślnie wszystkie kopie zapasowe będą pełne). Tworząc plan tworzenia kopii zapasowych, w polu **Ścieżka** określ folder lokalny lub strefę Acronis Secure Zone. W obszarze **Reguły przechowywania** wybierz **Przeńszenie kopie zapasowe starsze niż 1 tydzień**. Następnie w polu **2. Lokalizacja** określ urządzenie taśmowe.

Sprawdź, czy urządzenie taśmowe jest gotowe. Czynności przygotowawcze zostały opisane w sekcji „Tworzenie kopii zapasowej komputera na bezpośrednio podłączonym urządzeniu taśmowym (s. 195)”.

Wynik:

- Po utworzeniu kopii zapasowej agent sprawdza, czy są kopie do przeniesienia.
- Agent przenosi kopie zapasowe starsze niż tydzień, kopiując je na urządzenie taśmowe, a następnie usuwając z lokalizacji oryginalnej.
- Po wykonaniu tej operacji można wyjąć taśmy z kopiami zapasowymi i zabezpieczyć je w innej lokalizacji. Po wybraniu danych do odzyskania program Acronis Backup & Recovery 11 poprosi o włożenie określonych taśm.

Przykład 4. Tworzenie kopii zapasowych na taśmach w krótkim czasie wyznaczonym na tworzenie kopii

W przykładzie założono korzystanie z zaawansowanej wersji programu Acronis Backup & Recovery 11.

Rozważmy następujący scenariusz:

- Chcesz tworzyć kopie zapasowe serwerów codziennie w dni robocze po godzinach pracy.
- Chcesz tworzyć miesięczną pełną kopię zapasową w jeden z dni roboczych, a w pozostałe dni robocze — kopie częściowe (przyrostowe lub różnicowe).
- Chcesz przechowywać kopie zapasowe na bibliotece taśm.
- Okno tworzenia kopii zapasowych dla serwerów jest wąskie, więc nie można ich zapisywać bezpośrednio na taśmach.

W tym scenariuszu należy zainstalować węzeł Acronis Backup & Recovery 11 Storage Node i utworzyć dwa skarbcze zarządzane: jeden na lokalnym dysku twardym węzła magazynowania i drugi na bibliotece taśm podłączonej bezpośrednio do niego.

Utwórz scentralizowany plan tworzenia kopii zapasowych dla wszystkich komputerów z wykorzystaniem schematu **Dziadek-ojciec-syn (GFS)**. Tworząc plan tworzenia kopii zapasowych, w polu **Ścieżka** określ skarbiec na dysku twardym. W obszarze **Typ kopii zapasowej** wybierz **Pełna/przyrostowa/różnicowa**.

W obszarze **Zachowuj kopie zapasowe** lokalizacji podstawowej wybierz miesięczne kopie zapasowe przechowywane przez jeden miesiąc (musisz anulować zaznaczenie pola wyboru **Zachowaj w nieskończoność**). Dzięki temu skarbiec będzie pełnił rolę pośredniego magazynu do krótkotrwałego przechowywania kopii zapasowych.

Zaznacz pole wyboru **Replikuj nowo utworzoną kopię zapasową do innej lokalizacji**, a następnie w polu **2. lokalizacja** określ skarbiec w bibliotece taśm. W przypadku drugiej lokalizacji wybierz opcję zachowywania miesięcznych kopii zapasowych w nieskończoność.

Wynik:

- Agenty będą tworzyły kopie zapasowe swoich komputerów w skarbcu na dysku twardym.
- Węzeł magazynowania kopiuje kopie zapasowe na urządzenie taśmowe. Proces ten nie będzie angażował zasobów procesorów na poszczególnych komputerach.
- Czas przechowywania kopii zapasowych na dysku twardym nie przekracza jednego miesiąca. W bibliotece taśm miesięczne kopie zapasowe będą przechowywane w nieskończoność.

4.6 Konfigurowanie regularnej konwersji na maszynę wirtualną

Podczas definiowania planu tworzenia kopii zapasowych (s. 48) można skonfigurować regularną konwersję kopii zapasowej dysku lub woluminu na maszynę wirtualną. Skonfigurowanie regularnej konwersji pozwala uzyskać kopię serwera lub stacji roboczej na maszynie wirtualnej, którą można szybko włączyć w przypadku awarii oryginalnego komputera.

Ograniczenia

- Konwersja jest niedostępna na komputerach z systemem Linux.
- Nie jest możliwa konwersja kopii zapasowej z następujących lokalizacji: płyt CD, DVD, urządzeń taśmowych oraz magazynu Acronis Online Backup Storage.
- Jeśli skonfigurowano kopiowanie lub przenoszenie kopii zapasowych do innych lokalizacji (s. 90), nie można skonfigurować konwersji z żadnej z tych lokalizacji. Konwersja jest zawsze wykonywana z pierwszej lokalizacji kopii zapasowej.

W poniższej sekcji znajdują się informacje ułatwiające wprowadzenie odpowiednich ustawień.

Konwersja na maszynę wirtualną

Czas przeprowadzenia konwersji

W zależności od wybranego schematu tworzenia kopii zapasowych określ, czy należy konwertować każdą pełną, przyrostową lub różnicową kopię zapasową, czy ostatnią utworzoną kopię zapasową według harmonogramu. W razie potrzeby określ **harmonogram konwersji (s. 100)**.

Przeglądaj (s. 100)

Określ komputer, który wykona konwersję. Na komputerze musi być zainstalowany komponent Acronis Backup & Recovery 11 Agent for ESX(i), Agent for Hyper-V lub Agent for Windows.

Konwersję można wykonać za pomocą agenta, który wykonuje kopię zapasową, lub za pomocą agenta zainstalowanego na innym komputerze. W tym drugim przypadku archiwum należy przechowywać w lokalizacji udostępnionej, takiej jak folder sieciowy lub skarboniec zarządzany. Dzięki temu drugi komputer będzie miał dostęp do archiwum.

Typ maszyny wirtualnej (s. 160)

W tym miejscu można wybrać typ i lokalizację wynikowej maszyny wirtualnej. Dostępne opcje zależą od hosta wybranego w poprzednim kroku.

Magazyn

Wybierz magazyn na serwerze wirtualizacji lub folder, w którym zostaną umieszczone pliki maszyny wirtualnej.

Wynikowe maszyny wirtualne

Określ nazwę maszyny wirtualnej. Domyślna nazwa to **Kopia_zapasowa_z_[Nazwa maszyny]**. Można ją uzupełnić o dodatkowe zmienne. Obsługiwane są następujące szablony:

[Nazwa planu]

[Nazwa maszyny]

[Nazwa hosta wirtualnego]

[Nazwa maszyny wirtualnej]

[Typ serwera wirtualizacji]

Folder w VMware vCenter

Jeśli serwer zarządzania jest zintegrowany z serwerem vCenter Server, wynikowe maszyny wirtualne pojawią się w folderze **Acronis Backups** na serwerze vCenter. Dla maszyn tworzonych w wyniku wykonywania planu można określić podfolder.

4.6.1 Konfigurowanie harmonogramu konwersji

Kopię zapasową dysku (s. 381) utworzoną wskutek wykonania planu tworzenia kopii zapasowych można przekonwertować na maszynę wirtualną — natychmiast, zgodnie z harmonogramem lub przy użyciu obu tych metod.

Zadanie konwersji zostanie utworzone na komputerze, którego dotyczy tworzenie kopii zapasowej, i użyje daty oraz godziny tego komputera. Jeśli agent tworzący kopię zapasową komputera jest zainstalowany poza nim (na przykład w przypadku tworzenia kopii zapasowej maszyny wirtualnej ESX(i) lub Hyper-V na poziomie hiperwizora), zadanie zostanie utworzone na komputerze z agentem.

W momencie uruchomienia konwersji docelowa maszyna wirtualna musi być wyłączona. W przeciwnym razie zadanie konwersji nie powiedzie się. W takiej sytuacji należy wyłączyć maszynę i ręcznie ponownie uruchomić zadanie konwersji. Wszystkie zmiany wprowadzone we włączonej maszynie zostaną zastąpione.

4.6.2 Wybieranie komputera, który przeprowadzi konwersję

Należy rozważyć poniższe czynniki.

Jaki agent jest zainstalowany na komputerze?

Typ i lokalizacja wynikowej maszyny wirtualnej zależą od agenta znajdującego się na wybranym komputerze.

- Na komputerze jest zainstalowany **agent dla ESX(i)**

Jeśli agent zarządza więcej niż jednym hostem ESX(i), można wybrać hosta, na którym zostanie utworzona maszyna wirtualna. Takiego wyboru dokonuje się w kroku **Typ maszyny wirtualnej** (s. 160).

W kroku **Pamięć masowa** można określić pamięć masową, w której zostanie utworzona maszyna wirtualna.

Do planu tworzenia kopii zapasowych nie można dodawać maszyn wirtualnych utworzonych w wyniku utworzenia kopii zapasowej. Na serwerze zarządzania są one wyświetlane jako niezarządzane lub nie pojawiają się w ogóle (jeśli nie jest włączona integracja z serwerem vCenter).

- Na komputerze jest zainstalowany **agent dla Hyper-V**

Można utworzyć maszynę wirtualną na serwerze Hyper-V albo maszynę wirtualną VMware Workstation, Microsoft Virtual PC lub Parallels Workstation. Takiego wyboru dokonuje się w kroku **Typ maszyny wirtualnej** (s. 160).

W kroku **Pamięć masowa** można określić ścieżkę do maszyny wirtualnej.

Maszyny wirtualne utworzone na serwerze w wyniku utworzenia kopii zapasowej nie pojawiają się na serwerze zarządzania. Wynika to z faktu, że maszyny tego typu nie powinny być umieszczane w kopiach zapasowych.

- Na komputerze jest zainstalowany komponent **agent dla systemu Windows**

Dostępne są następujące typy maszyn wirtualnych: VMware Workstation, Microsoft Virtual PC lub Parallels Workstation. Takiego wyboru dokonuje się w kroku **Typ maszyny wirtualnej** (s. 160). W kroku **Pamięć masowa** można określić ścieżkę do maszyny wirtualnej.

Jaka jest moc obliczeniowa komputera?

Konwersja zajmie zasoby procesora wybranego komputera. Na komputerze tym może powstać kolejka wielu zadań konwersji. Ich wykonanie może zająć dużo czasu. Weź to pod uwagę podczas tworzenia scentralizowanego planu tworzenia kopii zapasowych z konwersją wielu komputerów lub tworzenia wielu lokalnych planów tworzenia kopii zapasowych wykorzystujących do konwersji ten sam komputer.

Jaki magazyn będzie używany przez maszyny wirtualne?

Wykorzystanie sieci

W przeciwieństwie do zwykłych kopii zapasowych (plików TIB) pliki maszyn wirtualnych są przesyłane przez sieć w postaci nieskompresowanej. Oznacza to, że z punktu widzenia wykorzystania sieci optymalnym rozwiązaniem jest użycie sieci SAN lub magazynu lokalnego względem komputera, który wykonuje konwersję. Jeśli jednak konwersję wykonuje ten sam komputer, którego dotyczy operacja tworzenia kopii zapasowej, nie można użyć dysku lokalnego. Warto wówczas skorzystać z urządzenia NAS.

Miejsce do przechowywania

Dyski wynikowej maszyny wirtualnej zajmą tyle miejsca, ile zajmują oryginalne dane. Jeśli oryginalny dysk ma pojemność 100 GB i zawiera 10 GB danych, odpowiadający mu dysk wirtualny zajmie około 10 GB. W terminologii VMware format ten określa się terminem „alokowania elastycznego”, a w firmie Microsoft używa się pojęcia „dysku powiększającego się dynamicznie”.

Ponieważ miejsce nie jest wstępnie przydzielane, w magazynie fizycznym powinno być dosyć wolnego miejsca na zwiększenie rozmiarów dysków wirtualnych.

4.6.3 Zasada działania zwykłej konwersji na maszynę wirtualną (VM)

Zasada działania cyklicznych konwersji zależy od wybranego miejsca utworzenia maszyny wirtualnej.

- **Po wybraniu opcji zapisu maszyny wirtualnej w postaci zestawu plików:** każda konwersja spowoduje 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, a jedynie aktualizuje istniejącą maszynę. Taka konwersja trwa zwykle krócej. Wymaga ona przesłania przez sieć mniejszej ilości danych i mniej obciąża procesor hosta 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. Na początku tworzona jest nowa (tymczasowa) maszyna wirtualna. Jeśli ta operacja zakończy się powodzeniem, poprzednia maszyna jest zastępowana. Jeśli w czasie tworzenia tymczasowej maszyny wystąpi błąd, jest ona usuwana.

Oznacza to, że rezultatem konwersji zawsze jest jedna maszyna wirtualna. Jednak podczas konwersji wymagane jest dodatkowe miejsce, tak aby zmieściła się także maszyna tymczasowa.

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 utworzona ponownie od podstaw. Operacja ta obejmuje utworzenie tymczasowej maszyny wirtualnej zgodnie z wcześniejszym opisem.
- 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

Aktualizacja maszyny wirtualnej wymaga zapisania przez program kilku jej migawek pośrednich. Mają one nazwy **Backup...** oraz **Replica...** i nie należy ich usuwać. Niepotrzebne migawki są usuwane automatycznie.

Ostatnia migawka **Replica** odpowiada wynikowi najnowszej konwersji. Można z niej skorzystać w celu przywrócenia maszyny do jej ostatniego stanu, na przykład do odrzucenia wprowadzonych zmian po zakończeniu pracy z maszyną.

Pozostałe migawki są przeznaczone do użytku wewnętrznego przez program.

4.7 Domyślne opcje tworzenia kopii zapasowej

Każdy agent Acronis ma swoje własne domyślne opcje tworzenia kopii zapasowych. Po jego zainstalowaniu domyślne opcje mają wstępnie zdefiniowane wartości określone w dokumentacji jako **ustawienia wstępne**. Podczas tworzenia planu tworzenia kopii zapasowych można użyć opcji domyślnej lub zastąpić tę opcję wartością niestandardową stosowaną tylko w odniesieniu do tego planu.

Można również dostosować opcję domyślną, zmieniając jej wartość na inną niż wstępnie zdefiniowana. Od tej pory program będzie domyślnie używał nowej wartości we wszystkich planach tworzenia kopii zapasowych tworzonych na danym komputerze.

Aby wyświetlić i zmienić domyślne opcje tworzenia kopii zapasowych, podłącz konsolę do komputera zarządzanego i z górnego menu wybierz **Opcje > Domyślne opcje tworzenia kopii zapasowej i odzyskiwania > Domyślne opcje tworzenia kopii zapasowej**.

Dostępne opcje tworzenia kopii zapasowych

Zakres dostępnych opcji tworzenia kopii zapasowych zależy od następujących czynników:

- Środowisko działania agenta (Windows, Linux, nośnik startowy).
- Typ danych umieszczanych w kopii zapasowej (dysk, plik).
- Miejsce docelowe kopii zapasowej (lokalizacja sieciowa lub dysk lokalny).
- Schemat tworzenia kopii zapasowych (uruchamianie ręczne lub przy użyciu harmonogramu).

W poniższej tabeli zestawiono dostępność opcji tworzenia kopii zapasowych.

	Agent dla systemu Windows		Agent dla systemu Linux		Nośnik startowy (oparty na systemie Linux lub na środowisku PE)	
	Kopia zapasowa dysku	Kopia zapasowa plików	Kopia zapasowa dysku	Kopia zapasowa plików	Kopia zapasowa dysku	Kopia zapasowa plików
Ustawienia dodatkowe (s. 105):						
W przypadku tworzenia kopii zapasowej na nośnikach wymiennych zapytaj o pierwszy nośnik	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny
Użyj usługi FTP w trybie aktywnym	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP
Deduplikuj kopie zapasowe po przetransferowaniu ich do skarbca	Miejsce docelowe: skarbiec deduplikacji	Miejsce docelowe: skarbiec deduplikacji	Miejsce docelowe: skarbiec deduplikacji	Miejsce docelowe: skarbiec deduplikacji	Miejsce docelowe: skarbiec deduplikacji	Miejsce docelowe: skarbiec deduplikacji
Resetuj bit archiwum	-	+	-	-	-	+
Ponownie uruchom komputer po utworzeniu kopii zapasowej	-	-	-	-	+	+
Ochrona archiwum (s. 107) (hasło + szyfrowanie)	+	+	+	+	+	+
Katalogowanie kopii zapasowej (s. 108)	+	+	+	+	-	-
Wydajność tworzenia kopii zapasowej:						
Priorytet tworzenia kopii zapasowej (s. 108)	+	+	+	+	-	-
Prędkość zapisu na dysku twardym (s. 109)	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy
Szybkość połączenia sieciowego (s. 109)	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy
Dzielenie kopii zapasowej (s. 109)	+	+	+	+	+	+
Stopień kompresji (s. 110)	+	+	+	+	+	+
Plan odzyskiwania po awarii (s. 111)	+	+	+	+	-	-
Obsługa błędów (s. 112):						
Nie pokazuj komunikatów ani okien	+	+	+	+	+	+

	Agent dla systemu Windows		Agent dla systemu Linux		Nośnik startowy (oparty na systemie Linux lub na środowisku PE)	
	Kopia zapasowa dysku	Kopia zapasowa plików	Kopia zapasowa dysku	Kopia zapasowa plików	Kopia zapasowa dysku	Kopia zapasowa plików
dialogowych podczas przetwarzania (tryb dyskretny)						
W przypadku wystąpienia błędu spróbuj ponownie	+	+	+	+	+	+
Ignoruj sektory uszkodzone	+	+	+	+	+	+
Śledzenie zdarzeń:						
Dziennik zdarzeń systemu Windows (s. 113)	+	+	-	-	-	-
SNMP (s. 113)	+	+	+	+	-	-
Szybka przyrostowa/różnicowa kopia zapasowa (s. 114)	+	-	+	-	+	-
Migawka kopii zapasowej na poziomie pliku (s. 114)	-	+	-	+	-	-
Zabezpieczenia na poziomie plików (s. 115):						
Zachowaj ustawienia zabezpieczeń plików w archiwach	-	+	-	-	-	-
Pliki zaszyfrowane zapisz w archiwach w postaci odszyfrowanej	-	+	-	-	-	-
Wykonywanie migawek LVM (s. 115)	-	-	+	-	-	-
Komponenty na nośniku (s. 116)	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	-	-
Punkty zamontowania (s. 117)	-	+	-	-	-	-
Migawka wielowoluminowa (s. 117)	+	+	-	-	-	-
Powiadomienia:						
E-mail (s. 118)	+	+	+	+	-	-
WinPopup (s. 119)	+	+	+	+	-	-

	Agent dla systemu Windows		Agent dla systemu Linux		Nośnik startowy (oparty na systemie Linux lub na środowisku PE)	
	Kopia zapasowa dysku	Kopia zapasowa plików	Kopia zapasowa dysku	Kopia zapasowa plików	Kopia zapasowa dysku	Kopia zapasowa plików
Polecenia poprzedzające tworzenie kopii zapasowej/następujące po nim (s. 119)	+	+	+	+	Tylko PE	Tylko PE
Polecenia poprzedzające rejestrowanie danych/następujące po nim (s. 121)	+	+	+	+	-	-
Czas braku aktywności replikacji/czyszczenia (s. 96)	+	+	+	+	-	-
Kopia zapasowa sektor po sektorze (s. 124)	+	-	+	-	+	-
Zarządzanie taśmami (s. 124)	Miejsce docelowe: taśma	Miejsce docelowe: taśma	Miejsce docelowe: taśma	Miejsce docelowe: taśma	Miejsce docelowe: taśma	Miejsce docelowe: taśma
Obsługa niepowodzenia zadania (s. 125)	+	+	+	+	-	-
Warunki uruchomienia zadania (s. 126)	+	+	+	+	-	-
Usługa kopiowania woluminów w tle (s. 127)	+	+	-	-	-	-

4.7.1 Ustawienia dodatkowe

Określ dodatkowe ustawienia operacji tworzenia kopii zapasowej, zaznaczając lub czyszcząc poniższe pola wyboru.

W przypadku tworzenia kopii zapasowej na nośnikach wymiennych zapytaj o pierwszy nośnik

Ta opcja jest dostępna tylko podczas tworzenia kopii zapasowej na nośniku wymiennym.

Określa ona, czy podczas tworzenia kopii zapasowej na nośniku wymiennym ma być wyświetlany monit **Włóż pierwszy nośnik**.

Ustawienie wstępne: **Włączone**.

Gdy opcja jest włączona, a użytkownik nie znajduje się w pobliżu komputera, utworzenie kopii zapasowej na nośniku wymiennym może okazać się niemożliwe, ponieważ program będzie czekał na kliknięcie przycisku OK w oknie monitu. Dlatego, jeśli planujesz w harmonogramie tworzenie kopii zapasowej na nośniku wymiennym, wyłącz wyświetlanie monitu. W takiej sytuacji, jeśli nośnik

wymienny będzie dostępny (na przykład włożona będzie płyta DVD), zadanie będzie kontynuowane bez udziału użytkownika.

Resetuj bit archiwum

Ta opcja jest dostępna tylko w przypadku kopii zapasowej na poziomie plików w systemach operacyjnych Windows i na nośniku startowym.

Ustawienie wstępne: **Wyłączone**.

W systemach operacyjnych Windows każdy plik ma atrybut **Plik jest gotowy do archiwizacji**, dostępny po wybraniu **Plik** -> **Właściwości** -> **Ogólne** -> **Zaawansowane** -> **Atrybuty archiwizacji i indeksowania**. W systemie operacyjnym ten atrybut — zwany również bitem archiwum — jest ustawiany przy każdej zmianie pliku, a aplikacje do tworzenia kopii zapasowych mogą go przestawiać za każdym razem, gdy umieszczają plik w kopii zapasowej. Wartość bitu archiwum jest używana przez różne aplikacje, na przykład bazy danych.

Gdy pole wyboru **Resetuj bit archiwum** jest zaznaczone, program Acronis Backup & Recovery 11 zresetuje bity archiwum wszystkich plików umieszczanych w kopii zapasowej. Program Acronis Backup & Recovery 11 sam w sobie nie korzysta z wartości bitu archiwum. Podczas tworzenia przyrostowej lub różnicowej kopii zapasowej program ustala, czy plik się nie zmienił, na podstawie rozmiaru pliku i daty/godziny jego ostatniego zapisu.

Ponownie uruchom komputer po utworzeniu kopii zapasowej

Ta opcja jest dostępna tylko podczas pracy z nośnikiem startowym.

Ustawienie wstępne: **Wyłączone**.

Gdy opcja jest włączona, po utworzeniu kopii zapasowej program Acronis Backup & Recovery 11 ponownie uruchomi komputer.

Jeśli na przykład komputer jest domyślnie uruchamiany z dysku twardego i to pole jest zaznaczone, niezwłocznie po utworzeniu kopii zapasowej przez agenta komputer zostanie ponownie uruchomiony i rozpocznie się ładowanie systemu operacyjnego.

Deduplikuj kopie zapasowe po przetransferowaniu ich do skarbca (nie deduplikuj w miejscu źródłowym)

Ta opcja jest dostępna tylko w zaawansowanych wersjach programu Acronis Backup & Recovery 11.

Ta opcja jest dostępna w przypadku systemów operacyjnych Windows i Linux oraz nośnika startowego, gdy miejscem docelowym kopii zapasowej jest skarbiec deduplikacji.

Ustawienie wstępne: **Wyłączone**.

Włączenie tej opcji powoduje wyłączenie deduplikacji kopii zapasowych w źródle, co oznacza, że deduplikacja będzie wykonywana w węźle magazynowania Acronis Backup & Recovery 11 Storage Node po zapisaniu kopii zapasowej w skarbcu (jest to czynność nazywana deduplikacją w miejscu docelowym).

Wyłączenie deduplikacji w źródle może przyspieszyć tworzenie kopii zapasowych, ale jednocześnie spowodować większy ruch w sieci i obciążenie węzła magazynowania. Ostateczny rozmiar kopii zapasowej w skarbcu jest niezależny od tego, czy deduplikacja w źródle jest włączona.

Opis deduplikacji w źródle i deduplikacji w miejscu docelowym znajduje się w sekcji Omówienie deduplikacji (s. 224).

Użyj usługi FTP w trybie aktywnym

Ustawienie wstępne: **Wyłączone**.

Włącz tę opcję, jeśli serwer FTP obsługuje tryb aktywny i chcesz go używać do przesyłania plików.

4.7.2 Ochrona archiwum

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux oraz w przypadku nośników startowych.

Ta opcja jest dostępna zarówno podczas tworzenia kopii zapasowej na poziomie dysku, jak i kopii zapasowej na poziomie plików.

Ta opcja określa, czy archiwum będzie chronione hasłem, i czy jego zawartość będzie szyfrowana.

Jest ona niedostępna, jeśli archiwum zawiera już kopie zapasowe. Opcja ta może być niedostępna na przykład:

- Jeśli jako lokalizację docelową planu tworzenia kopii zapasowych określisz już istniejące archiwum.
- Jeśli wyedytujesz plan tworzenia kopii zapasowych, w wyniku działania którego powstała już kopia zapasowa.

Ustawienie wstępne: **Wyłączone**.

Aby zabezpieczyć archiwum przed nieuprawnionym dostępem

1. Zaznacz pole wyboru **Ustaw hasło do archiwum**.
2. W polu **Wprowadź hasło** wpisz hasło.
3. W polu **Potwierdź hasło** wpisz ponownie hasło.
4. Wybierz jedną z następujących opcji:
 - **Nie szyfruj** — archiwum będzie chronione jedynie hasłem.
 - **AES 128** — archiwum zostanie zaszyfrowane przy użyciu algorytmu Advanced Encryption Standard (AES) z kluczem 128-bitowym.
 - **AES 192** — archiwum zostanie zaszyfrowane przy użyciu algorytmu AES z kluczem 192-bitowym.
 - **AES 256** — archiwum zostanie zaszyfrowane przy użyciu algorytmu AES z kluczem 256-bitowym.
5. Kliknij **OK**.

Algorytm kryptograficzny AES działa w trybie wiązania bloków szyfrogramu (Cipher-Block Chaining — CBC) i korzysta z losowo wygenerowanego klucza o długości zdefiniowanej przez użytkownika: 128, 192 lub 256 bitów. Im większy rozmiar klucza, tym dłużej trwa szyfrowanie archiwum, ale dane są lepiej zabezpieczone.

Klucz szyfrowania jest następnie szyfrowany metodą AES-256, w której jako klucz służy skrót SHA-256 hasła. Same hasło nie jest przechowywane w żadnym miejscu na dysku ani w pliku kopii zapasowej — do celów weryfikacji służy skrót hasła. Dzięki tym dwupoziomowym zabezpieczeniom dane kopii zapasowej są chronione przed nieautoryzowanym dostępem, ale odzyskanie utraconego hasła jest niemożliwe.

4.7.3 Katalogowanie kopii zapasowej

Katalogowanie kopii zapasowej powoduje dodanie jej zawartości do wykazu danych. Wykaz danych ułatwia znalezienie wymaganej wersji danych i wybranie ich do odzyskania.

Opcja **Katalogowanie kopii zapasowej** określa, czy kopie zapasowe będą katalogowane automatycznie natychmiast po utworzeniu.

Ustawienie wstępne: **Włączone**.

Po ukończeniu procesu katalogowania w wykazie znajdą się wszystkie dane zawarte w nowo utworzonej kopii zapasowej:

- W przypadku kopii zapasowej na poziomie dysku — dyski, woluminy, pliki i foldery.
- W przypadku kopii zapasowej na poziomie pliku — pliki i foldery.

Opcję automatycznego katalogowania warto wyłączyć, jeśli wpływa ona na wydajność komputera zarządzanego lub gdy okno tworzenia kopii zapasowych jest zbyt wąskie. Jeśli opcja **Katalogowanie kopii zapasowej** jest wyłączona, w wykazie znajdą się następujące dane:

- W przypadku kopii zapasowej na poziomie dysku — tylko dyski i woluminy.
- W przypadku kopii zapasowej na poziomie pliku — brak.

Aby dodać do wykazu pełną zawartość wcześniej utworzonych kopii zapasowych, proces katalogowania można uruchomić ręcznie w dogodnym czasie.

Aby uzyskać więcej informacji na temat korzystania z wykazu danych, zobacz Wykaz danych (s. 134).

4.7.4 Wydajność tworzenia kopii zapasowej

Ta grupa opcji umożliwia określenie ilości zasobów sieciowych i systemowych przydzielonych do procesu tworzenia kopii zapasowej.

Opcje wydajności tworzenia kopii zapasowej mogą mieć większy lub mniejszy wpływ na szybkość tworzenia kopii zapasowej. Zależy to od ogólnej konfiguracji systemu i fizycznej charakterystyki urządzeń biorących udział w procesie tworzenia kopii zapasowej.

Priorytet tworzenia kopii zapasowej

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Priorytet procesu uruchomionego w systemie określa ilość zasobów procesora i systemu przydzielonych do tego procesu. Zmniejszenie priorytetu procesu tworzenia kopii zapasowej spowoduje zwolnienie większej ilości zasobów dla innych aplikacji. Zwiększenie priorytetu procesu tworzenia kopii zapasowej może go przyspieszyć dzięki przydzieleniu większej ilości zasobów, np. procesora, dla aplikacji do tworzenia kopii zapasowej. Końcowy efekt zależy jednak od ogólnego obciążenia procesora i innych czynników, takich jak prędkość zapisu/odczytu dysków i obciążenie sieci.

Ustawienie wstępne: **Niski**.

Aby określić priorytet procesu tworzenia kopii zapasowej

Wybierz jedną z następujących opcji:

- **Niski** — minimalizuje ilość zasobów wykorzystywanych przez proces tworzenia kopii zapasowej, pozostawiając więcej zasobów dla innych procesów uruchomionych na komputerze

- **Normalny** — proces tworzenia kopii zapasowej działa z normalną prędkością, wykorzystując podobną ilość zasobów jak inne procesy
- **Wysoki** — proces tworzenia kopii zapasowej działa z maksymalną prędkością, wykorzystując zasoby, które były używane przez inne procesy

Prędkość zapisu na dysku twardym

Ta opcja jest dostępna w przypadku systemów operacyjnych Windows i Linux oraz nośnika startowego.

Opcja jest dostępna, gdy jako miejsce docelowe kopii zapasowej został wybrany wewnętrzny dysk twardy komputera, którego kopia zapasowa jest tworzona.

Tworzenie kopii zapasowej na stałym dysku twardym (na przykład w strefie Acronis Secure Zone) może spowolnić działanie systemu operacyjnego i aplikacji z powodu dużej ilości danych zapisywanych na dysku. Wykorzystanie dysku twardego w procesie tworzenia kopii zapasowej można ograniczyć do odpowiedniego poziomu.

Ustawienie wstępne: **Maksymalna**.

Aby ustawić żądaną prędkość zapisu na dysku twardym w procesie tworzenia kopii zapasowej

Wykonaj jedną z następujących czynności:

- Kliknij **Prędkość zapisu określona jako wartość procentowa prędkości maksymalnej na docelowym dysku twardym** i przeciągnij suwak lub wybierz wartość procentową w polu.
- Kliknij **Prędkość zapisu wyrażona w kilobajtach na sekundę** i wprowadź prędkość zapisu w kilobajtach na sekundę.

Szybkość połączenia sieciowego

Ta opcja jest przeznaczona dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Ta opcja jest dostępna po wybraniu lokalizacji sieciowej (udziału sieciowego, zarządzanego skarbca lub serwera FTP/SFTP) jako miejsca docelowego dla kopii zapasowej.

Opcja określa wartość przepustowości łącza sieciowego przeznaczoną do przesyłania kopiowanych danych.

Domyślnie jest ustawiona maksymalna prędkość, tzn. oprogramowanie używa pełnej przepustowości podczas przesyłania danych kopii zapasowej. Ta opcja umożliwia zarezerwowanie pewnej przepustowości dla innych aplikacji sieciowych.

Ustawienie wstępne: **Maksymalna**.

Aby ustawić prędkość połączenia sieciowego dla tworzenia kopii zapasowej

Wykonaj jedną z następujących czynności:

- Kliknij **Prędkość transferu określona jako wartość procentowa szacowanej prędkości maksymalnej połączenia sieciowego**, i przeciągnij suwak lub wpisz wartość procentową w polu.
- Kliknij **Prędkość transferu wyrażona w kilobajtach na sekundę**, a następnie wprowadź limit przepustowości dla przesyłania danych kopii zapasowej w kilobajtach na sekundę.

4.7.5 Dzielenie kopii zapasowej

Ta opcja jest przeznaczona dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Ta opcja umożliwia zdefiniowanie sposobu dzielenia kopii zapasowej.

Ustawienie wstępne: **Automatycznie**.

Dostępne są następujące ustawienia.

Automatycznie

Przy tym ustawieniu program Acronis Backup & Recovery 11 będzie działał w następujący sposób.

- **Podczas tworzenia kopii zapasowej na dysku twardym:**

Jeżeli system plików dysku docelowego dopuszcza szacowany rozmiar pliku, zostanie utworzony jeden plik kopii zapasowej.

Jeżeli system plików dysku docelowego nie dopuszcza szacowanego rozmiaru pliku, kopia zapasowa zostanie automatycznie podzielona na kilka plików. Taka sytuacja może wystąpić, jeżeli kopia zapasowa zostanie umieszczona na dysku z systemem plików FAT16 lub FAT32, które posiadają limit rozmiaru pliku 4 GB.

Jeżeli podczas tworzenia kopii zapasowej na dysku docelowym skończy się wolne miejsce, zadanie przejdzie w stan **Wymagające działania**. Można wówczas zwolnić dodatkowe miejsce na dysku i ponowić operację. W takim przypadku kopia zapasowa zostanie podzielona na części utworzone przed ponowieniem operacji i po nim.

- **Podczas tworzenia kopii zapasowej na nośniku wymiennym** (płyta CD, DVD lub urządzenie taśmowe dołączone lokalnie do komputera zarządzanego):

Zadanie przejdzie w stan **Wymagające działania** i kiedy nośnik będzie pełny, użytkownik zostanie poproszony o kolejny.

Stały rozmiar

Wprowadź pożądany rozmiar pliku lub wybierz go z listy rozwijanej. Nastąpi podział kopii zapasowej na wiele plików o określonym rozmiarze. Ta funkcja przydaje się podczas tworzenia kopii zapasowej nagrywanej następnie na wielu płytach CD lub DVD. Można również podzielić kopię zapasową przeznaczoną na serwer FTP, ponieważ odzyskiwanie danych bezpośrednio z serwera FTP wymaga podzielenia kopii zapasowej na pliki o rozmiarze nie większym niż 2 GB.

4.7.6 Stopień kompresji

Ta opcja jest przeznaczona dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Określa ona poziom kompresji danych w tworzonej kopii zapasowej.

Ustawienie wstępne: **Normalna**.

Optymalny poziom kompresji danych zależy od typu danych dodawanych do kopii zapasowej. Na przykład nawet maksymalny poziom kompresji nie zmniejszy znacząco rozmiaru archiwum, jeśli zawiera ono głównie skompresowane pliki, takie jak .jpg, .pdf lub .mp3. Jednak pliki w formatach takich jak .doc lub .xls będą dobrze skompresowane.

Aby określić poziom kompresji

Wybierz jedną z następujących opcji:

- **Brak** — dane zostaną skopiowane bez kompresji. Otrzymana kopia zapasowa będzie miała maksymalny rozmiar.
- **Normalny** — ustawienie zalecane w większości przypadków.

- **Wysoka** — otrzymana kopia zapasowa będzie zazwyczaj mniejsza niż w przypadku użycia ustawienia **Normalna**.
- **Maksymalna** — dane zostaną skompresowane w maksymalnym stopniu. Czas tworzenia kopii zapasowej będzie najdłuższy. Maksymalny poziom kompresji należy wybierać w przypadku tworzenia kopii zapasowej na nośnikach wymiennych w celu zmniejszenia liczby wymaganych nośników.

4.7.7 Plan odzyskiwania po awarii (DRP)

Ta opcja ma zastosowanie w systemach Windows i Linux, ale nie obejmuje nośników startowych.

Plan odzyskiwania po awarii (DRP) obejmuje listę uwzględnionych w kopii zapasowej elementów danych oraz szczegółowe instrukcje prowadzące użytkownika przez proces odzyskiwania tych elementów z kopii zapasowej.

Jeśli opcja **Plan odzyskiwania po awarii (DRP)** jest włączona, plan DRP zostanie utworzony i rozesłany pocztą e-mail do określonej listy użytkowników po pierwszym pomyślnym wykonaniu kopii zapasowej w ramach planu tworzenia kopii zapasowych. Zostanie on ponownie utworzony i rozesłany po pierwszym pomyślnym wykonaniu kopii zapasowej w następujących przypadkach:

- Plan tworzenia kopii zapasowych został zmodyfikowany tak, że zmieniły się parametry planu DRP.
- Kopia zapasowa objęła nowe elementy danych lub przestała obejmować elementy wcześniej uwzględnione (nie dotyczy to takich elementów danych, jak pliki i foldery).

Jeśli wiele komputerów zostaje objętych planem tworzenia kopii zapasowych, osobny plan DRP jest wysyłany dla każdego komputera.

Polecenia DRP i polecenia następujące po tworzeniu kopii zapasowej

Należy zauważyć, że plan DRP nie zostanie automatycznie zmieniony po skopiowaniu lub przeniesieniu kopii zapasowych z lokalizacji oryginalnej przez polecenia następujące po tworzeniu kopii zapasowej. Plan DRP wskazuje jedynie lokalizacje określone w planie tworzenia kopii zapasowych.

Dodawanie informacji do szablonu DRP

Jeśli znasz języki XML i HTML, możesz dodawać do szablonu DRP dodatkowe informacje. Domyślne ścieżki do szablonu DRP mają następującą postać:

- **%ProgramFiles%\Acronis\BackupAndRecovery\drp.xml** — w 32-bitowych systemach Windows
- **%ProgramFiles(x86)%\Acronis\BackupAndRecovery\drp.xml** — w 64-bitowych systemach Windows
- **/usr/lib/Acronis/BackupAndRecovery/drp.xml** — w systemie Linux

Aby skonfigurować wysyłanie planów DRP:

1. Zaznacz pole wyboru **Wysyłaj plan odzyskiwania po awarii**.
2. W polu **Adres e-mail** wprowadź adres e-mail. Można wprowadzić kilka adresów e-mail oddzielonych średnikami.
3. [Opcjonalnie] Zmień domyślną wartość pola **Temat**, jeśli to konieczne.

Jeśli tworzysz kopie zapasowe wielu komputerów za pomocą pojedynczego scentralizowanego planu tworzenia kopii zapasowych i chcesz, aby każdy z użytkowników komputera otrzymał osobną wiadomość e-mail DRP dotyczącą tylko danego komputera:

- a. Za pomocą zmiennej **%MachineName%** zawrzyj w temacie wiadomości e-mail nazwę konkretnego komputera.

- b. Skonfiguruj serwer lub klienta pocztowego tak, aby filtrował lub przysyłał dalej wiadomości e-mail w zależności od zawartości pola **Temat**.
4. Wprowadź parametry dostępu do serwera SMTP. Aby uzyskać szczegółowe informacje, zobacz Powiadomienia pocztą e-mail (s. 170).
5. [Opcjonalnie] Kliknij **Wyślij próbną wiadomość e-mail**, aby sprawdzić, czy ustawienia są poprawne.

4.7.8 Obsługa błędów

Te opcje są dostępne w przypadku systemów operacyjnych Windows i Linux oraz nośnika startowego.

Umożliwiają one określenie sposobu obsługi błędów, które mogą wystąpić podczas tworzenia kopii zapasowej.

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)

Ustawienie wstępne: **Wyłączone**.

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.

W przypadku wystąpienia błędu spróbuj ponownie

Ustawienie wstępne: **Włączone**. **Liczba prób: 30**. **Odstęp między próbami: 30 sekund**.

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 sieciowa lokalizacja docelowa kopii zapasowej będzie niedostępna lub nieosiągalna, program będzie próbował nawiązać połączenie co 30 sekund, ale nie więcej niż 5 razy. Próby zostaną wstrzymane po wznowieniu połączenia LUB po wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

Ignoruj sektory uszkodzone

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest wyłączona, po każdym natrafieniu na uszkodzony sektor program wyświetli okno z prośbą o podjęcie decyzji, czy kontynuować, czy zatrzymać tworzenie kopii zapasowej. 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.

4.7.9 Śledzenie zdarzeń

Zdarzenia z dziennika dotyczące operacji tworzenia kopii zapasowych, które są wykonywane na komputerze zarządzanym, można duplikować w dzienniku zdarzeń aplikacji systemu Windows lub wysyłać do określonych menedżerów SNMP.

Dziennik zdarzeń systemu Windows

Ta opcja jest uwzględniana tylko w systemach operacyjnych Windows.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa, czy agenty działające na komputerze zarządzanym muszą rejestrować zdarzenia operacji tworzenia kopii zapasowych w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, uruchom program **eventvwr.exe** lub wybierz kolejno: **Panel sterowania > Narzędzia administracyjne > Podgląd zdarzeń**). Zarejestrowane zdarzenia można filtrować.

Ustawienie wstępne: **Użyj ustawień określonych w obszarze Komputer.**

Aby określić, czy zdarzenia operacji tworzenia kopii zapasowych mają być rejestrowane w dzienniku zdarzeń aplikacji systemu Windows:

Wybierz jedną z następujących opcji:

- **Użyj ustawień określonych w obszarze Komputer** — aby użyć ustawienia określonego dla komputera. Aby uzyskać więcej informacji, zapoznaj się z sekcją Opcje komputera.
- **Rejestruj zdarzenia następujących typów** — aby rejestrować zdarzenia operacji tworzenia kopii zapasowych w dzienniku zdarzeń aplikacji. Należy określić typy rejestrowanych zdarzeń:
 - **Wszystkie zdarzenia** — rejestrowane są wszystkie zdarzenia (informacje, ostrzeżenia i błędy)
 - **Błędy i ostrzeżenia**
 - **Tylko błędy**
- **Nie rejestruj** — aby wyłączyć rejestrowanie zdarzeń operacji tworzenia kopii zapasowych w dzienniku zdarzeń aplikacji.

Powiadomienia SNMP

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa, czy agenty działające na komputerze zarządzanym muszą wysyłać zdarzenia operacji tworzenia kopii zapasowych z dziennika do określonych menedżerów Simple Network Management Protocol (SNMP). Można wybrać typy wysyłanych zdarzeń.

Aby uzyskać szczegółowe informacje na temat programu Acronis Backup & Recovery 11, zobacz „Obsługa SNMP (s. 46)”.

Ustawienie wstępne: **Użyj ustawień określonych w obszarze Komputer.**

Aby wybrać, czy zdarzenia operacji tworzenia kopii zapasowych mają być wysyłane do menedżerów SNMP:

Wybierz jedną z następujących opcji:

- **Użyj ustawień określonych w obszarze Komputer** — aby użyć ustawienia określonego dla komputera. Aby uzyskać więcej informacji, zapoznaj się z sekcją Opcje komputera.
- **Wyślij osobne powiadomienie SNMP dla każdego zdarzenia tworzenia kopii zapasowej** — aby wysyłać informacje o zdarzeniach operacji tworzenia kopii zapasowych do określonych menedżerów SNMP.
 - **Typy wysyłanych zdarzeń** — wybierz typy wysyłanych zdarzeń: **Wszystkie zdarzenia, Błędy i ostrzeżenia** lub **Tylko błędy**.

- **Nazwa/adres IP serwera** — wpisz nazwę lub adres IP hosta, na którym jest uruchomiona aplikacja do zarządzania SNMP, do której chcesz przysyłać komunikaty.
- **Spółeczność** — wpisz nazwę społeczności SNMP, do której należy host z aplikacją do zarządzania SNMP oraz komputer wysyłający. Typowe ustawienie to „publiczna”.

Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy ustawienia są poprawne.

- **Nie wysyłaj powiadomień SNMP** — aby wyłączyć wysłanie zdarzeń z dziennika dotyczących operacji tworzenia kopii zapasowych do menedżerów SNMP.

4.7.10 Szybka przyrostowa/różnicowa kopia zapasowa

Ta opcja jest przeznaczona dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Ta opcja jest uwzględniana podczas tworzenia przyrostowych i różnicowych kopii zapasowych na poziomie dysku.

Określa ona, czy zmiana w pliku jest określana na podstawie jego rozmiaru i daty utworzenia, czy na podstawie porównania zawartości z plikiem zapisanym w archiwum.

Ustawienie wstępne: **Włączone**.

Przyrostowe i różnicowe kopie zapasowe umożliwiają zapisanie jedynie zmienionych danych. Aby przyspieszyć proces tworzenia kopii zapasowej, program określa, czy dany plik uległ modyfikacji na podstawie jego rozmiaru i daty oraz godziny zapisania. Wyłączenie tej funkcji spowoduje, że program będzie porównywał całą zawartość plików z plikami zapisanymi w archiwum.

4.7.11 Migawka kopii zapasowej na poziomie pliku

Ta opcja ma zastosowanie tylko w przypadku kopii zapasowych na poziomie pliku. Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux.

Ta opcja określa, czy kopia zapasowa ma być tworzona kolejno dla poszczególnych plików, czy też ma zostać utworzona migawka.

Uwaga: *Pliki zapisane w udostępnionych zasobach sieciowych są zawsze dodawane do kopii zapasowej kolejno.*

Ustawienie wstępne: **Utwórz migawkę, jeśli to możliwe**.

Wybierz jedną z następujących opcji:

- **Zawsze twórz migawkę**
Migawka umożliwia utworzenie kopii zapasowej wszystkich plików, w tym plików otwartych do wyłącznego dostępu. Kopia zapasowa plików zostanie utworzona w tym samym momencie. To ustawienie należy wybrać tylko wówczas, gdy czynniki te mają krytyczne znaczenie, tzn. utworzenie kopii zapasowej bez tworzenia migawki nie ma sensu. Aby użyć migawki, plan utworzenia kopii zapasowej musi być uruchomiony z konta z uprawnieniami administratora lub operatora kopii zapasowej. Jeśli nie można utworzyć migawki, utworzenie kopii zapasowej zakończy się niepowodzeniem.
- **Utwórz migawkę, jeśli to możliwe**
Jeśli nie można wykonać migawki, należy utworzyć bezpośrednią kopię zapasową plików.
- **Nie twórz migawki**
Zawsze wykonuj bezpośrednią kopię zapasową plików. Uprawnienia administratora lub operatora kopii zapasowej nie są wymagane. Próba utworzenia kopii zapasowej plików otwartych

do wyłącznego dostępu zakończy się błędem odczytu. Pliki w kopii zapasowej mogą być utworzone w różnych chwilach.

4.7.12 Zabezpieczenia na poziomie plików

Te opcje są uwzględniane tylko w przypadku kopii zapasowej na poziomie plików w systemach operacyjnych Windows.

Pliki zaszyfrowane zapisz w archiwach w postaci odszyfrowanej

Ta opcja umożliwia określenie, czy pliki mają być odszyfrowane przed zapisaniem ich w archiwum kopii zapasowej.

Ustawienie wstępne: **Wyłączone**.

Zignoruj tę opcję, jeżeli nie korzystasz z szyfrowania. Włącz tę opcję, jeżeli kopia zapasowa zawiera pliki zaszyfrowane, które po odzyskaniu mają być dostępne dla dowolnego użytkownika. W przeciwnym razie tylko użytkownik, który zaszyfrował pliki lub foldery, będzie mógł je odczytać. Odszyfrowanie może być również przydatne, jeżeli odzyskanie zaszyfrowanych plików następuje na innym komputerze.

*Funkcja szyfrowania plików jest dostępna w systemach Windows używających systemu plików NTFS z systemem szyfrowania plików (Encrypting File System). Aby uzyskać dostęp do ustawień szyfrowania plików lub folderów, wybierz **Właściwości** > **Ogólne** > **Atrybuty zaawansowane** > **Szyfruj zawartość, aby zabezpieczyć dane**.*

Zachowaj ustawienia zabezpieczeń plików w archiwach

Ta opcja pozwala określić, czy razem z kopią zapasową plików utworzyć również kopię zapasową uprawnień NTFS.

Ustawienie wstępne: **Włączone**.

Gdy opcja jest włączona, pliki i foldery są zapisywane w archiwum z oryginalnymi uprawnieniami odczytu, zapisu lub wykonywania plików każdego użytkownika lub grupy użytkowników. W przypadku odzyskiwania plików lub folderów na komputerze bez konta użytkownika określonego w uprawnieniach ich odczyt lub modyfikacja może okazać się niemożliwa.

Aby całkowicie wyeliminować ten problem, wyłącz zachowanie ustawień zabezpieczeń plików w archiwach. Odzyskane pliki i foldery zawsze otrzymają uprawnienia folderu, do którego zostaną odzyskane z dysku, jeżeli zostaną odzyskane do katalogu głównego.

Ewentualnie można wyłączyć odzyskiwanie (s. 169) ustawień zabezpieczeń, nawet jeżeli znajdują się w archiwum. Rezultat będzie taki sam — pliki otrzymają uprawnienia folderu nadrzędnego.

*Aby uzyskać dostęp do uprawnień NTFS pliku lub folderu, wybierz **Właściwości** > **Zabezpieczenia**.*

4.7.13 Wykonywanie migawek LVM

Ta opcja jest dostępna tylko w systemach operacyjnych Linux podczas tworzenia kopii zapasowych woluminów zarządzanych przez narzędzie Logical Volume Manager (LVM) systemu Linux. Woluminy takie określa się także mianem woluminów logicznych.

Opcja określa sposób wykonywania migawki woluminu logicznego i operowania nią. Użycie migawek gwarantuje powstanie spójnej czasowo kopii zapasowej woluminu, którego dane mogą zmieniać się w trakcie procesu tworzenia kopii.

Ustawienie wstępne: **Acronis Backup & Recovery 11**

Wskazówka: Zaleca się zmianę ustawienia wstępnego tylko w przypadku problemów z tworzeniem kopii zapasowych woluminów logicznych.

Możliwe są następujące ustawienia:

Acronis Backup & Recovery 11

Ustawienie Acronis Backup & Recovery 11 spowoduje zastosowanie własnego mechanizmu do wykonywania migawek i operowania nimi podczas tworzenia kopii zapasowych.

Menedżer woluminów logicznych

Ustawienie Acronis Backup & Recovery 11 spowoduje zastosowanie narzędzia Logical Volume Manager systemu Linux do wykonywania migawek i operowania nimi podczas tworzenia kopii zapasowych. Tworzenie kopii zapasowej woluminu w ten sposób może być mniej wydajne niż w przypadku wykorzystania mechanizmu Acronis.

Jeśli menedżer woluminów logicznych nie będzie mógł wykonać migawki, program Acronis Backup & Recovery 11 zastosuje ustawienie **Acronis Backup & Recovery 11**.

Jeśli operowanie wykonaną migawką zakończy się niepowodzeniem, nie będzie podejmowana próba wykonania dodatkowej migawki. Ma to zastosowanie do obu ustawień.

4.7.14 Komponenty na nośniku

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux, gdy miejscem docelowym kopii zapasowej jest nośnik wymienny.

Podczas tworzenia kopii zapasowej na nośniku wymiennym można przekształcić ten nośnik w zwykły nośnik startowy (s. 381) oparty na systemie Linux, dopisując do niego dodatkowe komponenty. Wskutek tego oddzielny dysk ratunkowy nie będzie potrzebny.

Ustawienie wstępne: **Brak komponentów startowych.**

Wybierz jeden z następujących komponentów, które chcesz umieścić na nośniku startowym:

- **Acronis Bootable Agent** to ratunkowe narzędzie startowe (oparte na jądrze systemu Linux), które zawiera większość funkcji agenta programu Acronis Backup & Recovery 11. Umieszczając ten komponent na nośniku, uzyskasz więcej funkcji podczas odzyskiwania. Operację odzyskiwania będzie można skonfigurować w taki sam sposób jak w przypadku zwykłego nośnika startowego. Użyj funkcji Active Restore lub Universal Restore. Jeśli nośnik jest tworzony w systemie Windows dostępna będzie także funkcja zarządzania dyskiem.
- **Acronis Bootable Agent i One-Click Restore.** One-Click Restore (przywracanie jednym kliknięciem) to minimalny dodatek do kopii zapasowej dysku przechowywanej na nośniku wymiennym, który umożliwia łatwe odzyskiwanie danych z kopii zapasowej. Po uruchomieniu komputera przy użyciu nośnika i kliknięciu opcji **Uruchom Acronis One-click Restore** dysk zostanie natychmiast odzyskany z kopii zapasowej zapisanej na tym samym nośniku.

Przestroga: Ponieważ metoda przywracania jednym kliknięciem nie przewiduje ustawień wybieranych przez użytkownika, takich jak określenie odzyskiwanych woluminów, funkcja Acronis One-Click Restore powoduje zawsze odzyskanie danych z całego dysku. Jeśli dysk zawiera kilka woluminów i planujesz korzystanie z

funkcji Acronis One-Click Restore, w kopii zapasowej uwzględnij wszystkie woluminy. Woluminy nieuwzględnione w kopii zapasowej zostaną utracone.

4.7.15 Punkty zamontowania

Ta opcja jest dostępna tylko w systemie Windows do tworzenia kopii zapasowej na poziomie pliku źródła danych obejmującego zamontowane woluminy lub woluminy udostępnione w klastrze.

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).

- Jeśli taki folder (folder nadrzędny) zostanie wybrany do utworzenia kopii zapasowej, a opcja **Punkty zamontowania** jest włączona, w kopii zapasowej będą uwzględnione wszystkie pliki znajdujące się w zamontowanym woluminie. Jeśli opcja **Punkty zamontowania** jest wyłączona, punkt zamontowania w kopii zapasowej będzie pusty.

Odzyskanie zawartości punktu zamontowania podczas odzyskiwania folderu nadrzędnego zależy od wartości opcji odzyskiwania **Punkty zamontowania** (s. 170).

- 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 odzyskiwania **Punkty dostępu** (s. 170).

Ustawienie wstępne: **Wyłączone**.

Wskazówka. Kopię zapasową maszyn wirtualnych Hyper-V znajdujących się w woluminie udostępnionym w klastrze tworzy się przez wykonanie kopii zapasowej na poziomie pliku wymaganych plików lub całego woluminu. Należy tylko pamiętać o wyłączeniu maszyn wirtualnych, aby ich kopia zapasowa była spójna.

Przykład

Przyjmijmy, że folder **C:\Dane1** to punkt zamontowania zamontowanego woluminu. Wolumin zawiera foldery **Folder1** i **Folder2**. Tworzysz plan tworzenia kopii zapasowej danych na poziomie pliku.

Jeśli zaznaczysz pole wyboru woluminu C i włączysz opcję **Punkty zamontowania**, folder **C:\Dane1** w kopii zapasowej będzie zawierać foldery **Folder1** i **Folder2**. Podczas odzyskiwania danych z kopii zapasowej należy pamiętać o poprawnym zastosowaniu opcji odzyskiwania **Punkty zamontowania** (s. 170).

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**, **Folder1** lub **Folder2**, zaznaczone foldery zostaną uwzględnione w kopii zapasowej jako zwykłe foldery bez względu na stan opcji **Punkty zamontowania**.

4.7.16 Migawka wielowoluminowa

Ta opcja ma zastosowanie tylko w systemach operacyjnych Windows..

Ta opcja dotyczy kopii zapasowej na poziomie dysku. Ma również zastosowanie w przypadku kopii zapasowej na poziomie pliku, gdy jest ona wykonywana przez utworzenie migawki. (Opcja Migawka

kopii zapasowej na poziomie pliku (s. 114) określa, czy podczas tworzenia kopii zapasowej na poziomie pliku zostanie utworzona migawka).

Opcja określa, czy migawki kilku woluminów mają być tworzone jednocześnie czy kolejno.

Ustawienie wstępne: **Włączone**.

Gdy opcja ta ma wartość **Włączone**, migawki wszystkich woluminów są tworzone jednocześnie. Opcji tej należy używać w celu utworzenia w jednej chwili kopii zapasowej danych na kilku woluminach, na przykład bazy danych Oracle.

Gdy opcja ta ma wartość **Wyłączone**, migawki woluminów będą tworzone kolejno. W efekcie, jeśli dane są rozłożone na kilku woluminach, kopia zapasowa może zawierać pliki utworzone w różnych chwilach.

4.7.17 Powiadomienia

Program Acronis Backup & Recovery 11 umożliwia powiadamianie użytkowników o utworzeniu kopii zapasowej przy użyciu poczty e-mail lub usługi komunikacyjnej.

E-mail

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja umożliwia odbieranie pocztą e-mail pełnego dziennika zadania oraz powiadomień o pomyślnym zakończeniu zadania utworzenia kopii zapasowej, niepowodzeniu wykonania zadania lub konieczności podjęcia działania.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować powiadamianie pocztą e-mail

1. Zaznacz pole wyboru **Wysyłaj powiadomienia pocztą e-mail**, aby włączyć powiadamianie.
2. W sekcji **Wysyłaj powiadomienia pocztą e-mail** zaznacz odpowiednie pola wyboru.
 - **Po pomyślnym utworzeniu kopii zapasowej** — aby wysłać powiadomienie po pomyślnym utworzeniu kopii zapasowej.
 - **Gdy utworzenie kopii zapasowej się nie powiedzie** — aby wysłać powiadomienie, gdy utworzenie kopii zapasowej nie powiedzie się.
 - **Gdy jest konieczne działanie użytkownika** — aby wysłać powiadomienie w czasie operacji, gdy wymagane jest podjęcie działania przez użytkownika.
3. Aby wiadomość e-mail zawierała wpisy dziennika związane z tworzeniem kopii zapasowej, zaznacz pole wyboru **Dodaj do powiadomienia pełny dziennik**.
4. W polu **Adresy e-mail** wpisz adres e-mail, na który będą wysyłane powiadomienia. Można wprowadzić kilka adresów oddzielonych średnikami.
5. W polu **Temat** wpisz temat wiadomości z powiadomieniem lub pozostaw wartość domyślną.
6. W polu **Serwer SMTP** wprowadź nazwę serwera SMTP.
7. W polu **Port** ustaw port serwera SMTP. Domyślnie jest to port **25**.
8. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika.
9. W polu **Hasło** wprowadź hasło.
10. Kliknij **Dodatkowe parametry poczty e-mail**, aby skonfigurować dodatkowe parametry poczty e-mail w następujący sposób:

- a. **Od** — wpisz adres e-mail użytkownika, od którego zostanie wysłana wiadomość. Jeśli pozostawisz to pole puste, wiadomości będą tworzone w taki sposób, jakby pochodziły z adresu docelowego.
- b. **Użyj szyfrowania** — umożliwia włączenie szyfrowanego połączenia z serwerem poczty. Można wybrać szyfrowanie SSL lub TLS.
- c. Niektórzy dostawcy usług internetowych umożliwiają wysłanie poczty dopiero po uwierzytelnieniu na serwerze poczty przychodzącej. Jeśli tak jest, zaznacz pole wyboru **Zaloguj się na serwerze poczty przychodzącej**, aby umożliwić korzystanie z serwera POP i skonfigurować jego ustawienia:
 - **Serwer poczty przychodzącej (POP)** — wprowadź nazwę serwera POP.
 - **Port** — ustaw port serwera POP. Domyślnie jest to port **110**.
 - **Nazwa użytkownika** — wprowadź nazwę użytkownika.
 - **Hasło** — wprowadź hasło.
- d. Kliknij **OK**.

11. Kliknij **Wyślij próbną wiadomość e-mail**, aby sprawdzić, czy ustawienia są poprawne.

Usługa Messenger (WinPopup)

Ta opcja działa w systemach operacyjnych Windows i Linux na komputerach wysyłających i tylko w systemie Windows na komputerach odbierających.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Opcja umożliwia odbieranie powiadomień WinPopup informujących o pomyślnym wykonaniu zadania, niepowodzeniu lub konieczności podjęcia działania.

Ustawienie wstępne: **Wyłączone**.

Przed skonfigurowaniem powiadomień WinPopup należy dopilnować, aby usługa Messenger była włączona na obu komputerach: wykonującym zadanie i odbierającym wiadomości.

Usługa Messenger nie jest domyślnie uruchamiana w systemach z grupy Microsoft Windows Server 2003. Zmień tryb uruchamiania usługi na Automatyczny i uruchom usługę.

Aby skonfigurować powiadomienia WinPopup:

1. Zaznacz pole wyboru **Wysyłaj powiadomienia WinPopup**.
2. W polu **Nazwa komputera** wprowadź nazwę komputera, do którego chcesz przysyłać powiadomienia. Używanie kilku nazw nie jest obsługiwane.

W sekcji **Wysyłaj powiadomienia** zaznacz odpowiednie pola wyboru

- **Po pomyślnym utworzeniu kopii zapasowej** — powiadomienie jest wysyłane po pomyślnym utworzeniu kopii zapasowej.
- **Gdy utworzenie kopii zapasowej się nie powiedzie** — powiadomienie jest wysyłane, gdy operacja tworzenia kopii zapasowej nie powiedzie się.
- **Gdy jest konieczne działanie użytkownika** — aby wysłać powiadomienie w czasie operacji, gdy wymagane jest podjęcie działania przez użytkownika.

Kliknij **Wyślij próbny komunikat WinPopup**, aby sprawdzić, czy ustawienia są poprawne.

4.7.18 Polecenia poprzedzające/następujące

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux oraz w przypadku nośników startowych opartych na środowisku PE.

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	Utworzenie kopii zapasowej	Polecenie następujące po utworzeniu kopii zapasowej
--	----------------------------	---

Przykłady zastosowania poleceń poprzedzających/następujących:

- usuwanie tymczasowych plików z dysku przed rozpoczęciem tworzenia kopii zapasowej.
- konfigurowanie produktów antywirusowych innych producentów w celu ich uruchomienia przed każdym rozpoczęciem tworzenia kopii zapasowej.
- kopiowanie i archiwizowanie w innej lokalizacji po utworzeniu kopii zapasowej.

Program nie obsługuje poleceń interaktywnych wymagających działania użytkownika (na przykład „pause”).

Aby określić polecenia poprzedzające/następujące

1. Włącz wykonywanie poleceń poprzedzających/następujących, zaznaczając następujące opcje:
 - **Wykonaj przed utworzeniem kopii zapasowej**
 - **Wykonaj po utworzeniu kopii zapasowej**
2. Wykonaj jedną z następujących czynności:
 - Kliknij **Edytuj**, aby określić nowe polecenie lub plik wsadowy.
 - Wybierz istniejące polecenie lub plik wsadowy z listy rozwijanej.
3. Kliknij **OK**.

Polecenie poprzedzające utworzenie kopii zapasowej

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu tworzenia kopii zapasowej

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy. Program nie obsługuje poleceń interaktywnych, to znaczy poleceń wymagających działania użytkownika (na przykład „pause”).
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Pole wyboru	Wybór			
Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie*	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. Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie.	Utwórz kopię zapasową po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N/D	Utwórz kopię zapasową równoległe z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.
--	---	--	-----	---

* Polecenie uznaje się za niewykonane, jeśli jego kod wyjścia jest różny od zera.

Polecenie następujące po utworzeniu kopii zapasowej

Aby określić polecenie/plik wykonywalny, które mają zostać wykonane po zakończeniu tworzenia kopii zapasowej

1. W polu **Polecenie** wpisz polecenie lub wyszukaj plik wsadowy.
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
4. Zaznacz pole wyboru **Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie**, jeśli pomyślne wykonanie polecenia ma znaczenie krytyczne. Polecenie uznaje się za niewykonane, jeśli jego kod wyjścia jest różny od zera. Jeśli wykonanie polecenia zakończy się niepowodzeniem, program usunie w miarę możliwości wynikowy plik TIB oraz pliki tymczasowe, a wynik wykonania zadania przyjmie wartość Zakończony niepowodzeniem.
 Jeśli to pole wyboru nie jest zaznaczone, wynik wykonania polecenia nie wpływa na powodzenie lub niepowodzenie wykonania zadania. Wynik wykonania polecenia można sprawdzić w dzienniku lub na liście błędów i ostrzeżeń wyświetlanej w widoku **Dziennik**.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest poprawne.

4.7.19 Polecenia poprzedzające rejestrowanie danych/następujące po nim

Ta opcja ma zastosowanie zarówno w systemach operacyjnych Windows, jak i Linux.

Ta opcja umożliwia określenie poleceń wykonywanych automatycznie przed zarejestrowaniem danych i po jego zakończeniu (czyli wykonaniu migawki danych). Migawka jest wykonywana przez program Acronis Backup & Recovery 11 na początku procedury tworzenia kopii zapasowej.

Poniższy schemat przedstawia czas wykonania poleceń poprzedzających i następujących po rejestrowaniu danych.

	<----- Kopia zapasowa ----->			
Polecenie poprzedzające utworzenie kopii zapasowej	Polecenie poprzedzające rejestrowanie danych	Rejestrowanie danych	Polecenie następujące po zarejestrowaniu danych	Polecenie następujące po utworzeniu kopii zapasowej

Jeśli opcja Usługa kopiowania woluminów w tle (s. 127) jest włączona, wykonywanie poleceń i czynności usługi Microsoft VSS odbędzie się w następującej kolejności:

Polecenia „Przed zarejestrowaniem danych” -> Wstrzymanie VSS -> Rejestrowanie danych -> Wznowienie VSS -> Polecenia „Po zarejestrowaniu danych”.

Przy użyciu poleceń wykonywanych przed rejestrowaniem danych lub po jego zakończeniu można zawiesić lub wznowić działanie bazy danych lub aplikacji, która nie jest kompatybilna z usługą VSS. W przeciwieństwie do poleceń poprzedzających/następujących (s. 119) polecenia poprzedzające rejestrowanie danych i następujące po nim są wykonywane przed procesem rejestrowania danych i po jego zakończeniu. Trwa to kilka sekund. Tworzenie kopii zapasowej może natomiast zająć dużo więcej czasu, w zależności od ilości danych. Dlatego czas przestoju bazy danych lub aplikacji jest minimalny.

Aby określić polecenia poprzedzające rejestrowanie danych/następujące po nim

1. Włącz wykonywanie poleceń poprzedzających rejestrowanie danych/następujących po nim, zaznaczając następujące opcje:
 - **Wykonaj przed zarejestrowaniem danych**
 - **Wykonaj po zarejestrowaniu danych**
2. Wykonaj jedną z następujących czynności:
 - Kliknij **Edytuj**, aby określić nowe polecenie lub plik wsadowy.
 - Wybierz istniejące polecenie lub plik wsadowy z listy rozwijanej.
3. Kliknij **OK**.

Polecenie poprzedzające rejestrowanie danych

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu rejestrowania danych

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy. Program nie obsługuje poleceń interaktywnych, to znaczy poleceń wymagających działania użytkownika (na przykład „pause”).
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Pole wyboru	Wybór			
	Wybrane	Niewybrane	Wybrane	Niewybrane
Zakończ niepowodzeniem tworzenie kopii zapasowej, jeśli wykonanie polecenia się nie powiedzie*				
Nie rejestruj danych przed zakończeniem wykonywania polecenia				
Wynik				
	Ustawienie wstępne Zarejestruj dane dopiero po pomyślnym wykonaniu polecenia. Zakończ zadanie niepowodzeniem, jeśli	Zarejestruj dane po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N/D	Zarejestruj dane równoległe z wykonywaniem polecenia i niezależnie od wyniku jego

	wykonanie polecenia się nie powiedzie.			wykonania.
--	--	--	--	------------

* Polecenie uznaje się za niewykonane, jeśli jego kod wyjścia jest różny od zera.

Polecenie następujące po zarejestrowaniu danych

Aby określić polecenie/plik wsadowy do wykonania po zarejestrowaniu danych

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy. Program nie obsługuje poleceń interaktywnych, to znaczy poleceń wymagających działania użytkownika (na przykład „pause”).
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Pole wyboru	Wybór			
Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie twórz kopii zapasowej przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Kontynuuj tworzenie kopii zapasowej dopiero po pomyślnym wykonaniu polecenia. Usuń plik TIB oraz pliki tymczasowe i zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia nie powiedzie się.	Kontynuuj tworzenie kopii zapasowej po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N/D	Kontynuuj tworzenie kopii zapasowej równoległe z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

* Polecenie uznaje się za niewykonane, jeśli jego kod wyjścia jest różny od zera.

4.7.20 Czas braku aktywności replikacji/czyszczenia

Ta opcja jest dostępna tylko w przypadku skonfigurowania reguł replikacji lub przechowywania (s. 90) kopii zapasowych.

Wskazuje ona okres, w którym nie można rozpocząć replikacji ani stosowania reguł przechowywania. Operacje te zostaną przeprowadzone po upływie czasu braku aktywności, jeśli komputer będzie wówczas włączony. Operacje uruchomione przed rozpoczęciem czasu braku aktywności będą kontynuowane bez przerwania.

Czas braku aktywności dotyczy wszystkich lokalizacji, w tym lokalizacji podstawowej.

Ustawienie wstępne: **Wyłączone**.

Aby określić czas braku aktywności, zaznacz pole wyboru **Nie rozpoczynaj replikacji/czyszczenia w następującym przedziale czasu**, a następnie wybierz dni oraz okres w ciągu dnia.

Przykład użycia

Warto użyć tej opcji do oddzielenia procesu tworzenia kopii zapasowej od zadań replikacji lub czyszczenia. Przyjmijmy, że tworzysz w trakcie dnia lokalne kopie zapasowe komputerów i replikujesz je do folderu sieciowego. Zdefiniuj czas braku aktywności tak, aby obejmował godziny pracy. Replikacja zostanie przeprowadzona po godzinach pracy, gdy obciążenie sieci jest niższe.

4.7.21 Kopia zapasowa sektor po sektorze

Ta opcja jest dostępna tylko w przypadku kopii zapasowych na poziomie dysku.

[Opcjonalnie] Aby utworzyć dokładną kopię dysku lub woluminu na poziomie fizycznym, zaznacz pole wyboru **Wykonaj kopię „sektor po sektorze”**. Wynikowa kopia zapasowa będzie tego samego rozmiaru co kopiowany dysk (jeśli **Stopień kompresji** (s. 110) ma ustawienie „Brak”). Operacja kopiowania „sektor po sektorze” pozwala tworzyć kopie zapasowe dysków zawierających nierozpoznane lub nieobsługiwane systemy plików oraz dane w innych zastrzeżonych formatach.

4.7.22 Zarządzanie taśmami

Opcje te mają zastosowanie, gdy miejscem docelowym kopii zapasowej jest urządzenie taśmowe.

Użyj oddzielnego zestawu taśm dla każdego komputera

Ustawienie wstępne: **Wyłączone**.

Taśmy w ramach jednej puli można pogrupować w postaci tzw. **zestawów taśm**.

Jeśli pozostawisz tę opcję wyłączoną, dane z różnych komputerów będą uwzględniane w tworzeniu kopii zapasowych na wszystkich taśmach należących do puli. Po włączeniu opcji kopie zapasowe każdego komputera będą przechowywane na osobnym zestawie taśm.

Opcja ma zastosowanie do tworzenia kopii zapasowych w węźle magazynowania.

Wysuń taśmę

Ustawienie wstępne: **Wyłączone**.

Jeśli to pole wyboru jest zaznaczone, program wysunie taśmę po pomyślnym utworzeniu kopii zapasowej lub po zapełnieniu taśmy.

Zawsze używaj wolnej taśmy

Domyślnie program próbuje zapisać kopię zapasową na taśmie zawierającej kopie zapasowe z tego samego ciągu lub archiwum. Jeśli nie zostanie ona znaleziona, program wyszuka taśmę z tego samego zestawu (zestawy taśm można określić za pomocą pul taśm, opcji **Użyj oddzielnego zestawu taśm dla każdego komputera** lub przy użyciu schematów Dziadek-ojciec-syn (GFS) (s. 56) albo Wieża Hanoi (s. 62)). Jeśli nie zostanie znaleziona taśma z tego samego zestawu, program spróbuje użyć wolnej taśmy.

Zmieniając następujące ustawienia, można wymusić użycie wolnej taśmy.

- **Do każdej pełnej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Po włączeniu tej opcji program zapisuje wszystkie pełne kopie zapasowe na wolnych taśmach.

- **Dla każdej różnicowej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest włączona, program zapisuje wszystkie różnicowe kopie zapasowe na wolnych taśmach. Ponadto program zapisuje wszystkie pełne kopie zapasowe na wolnych taśmach. Pole wyboru **Do każdej pełnej kopii zapasowej** zostanie zaznaczone i wyłączone.

- **Do każdej przyrostowej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest włączona, program zapisuje wszystkie przyrostowe kopie zapasowe na wolnych taśmach. Ponadto program zapisuje wszystkie pełne i przyrostowe kopie zapasowe na wolnych taśmach. Pola wyboru **Do każdej pełnej kopii zapasowej** i **Do każdej różnicowej kopii zapasowej** zostaną zaznaczone i wyłączone.

Zastąp taśmę w napędzie podczas tworzenia pełnej kopii zapasowej

Ustawienie wstępne: **Wyłączone**.

Opcja ma zastosowanie do autonomicznych napędów taśmowych. Gdy jest ona włączona, zawartość taśmy włożonej do napędu będzie zastąpiona za każdym utworzeniem pełnej kopii zapasowej.

4.7.23 Obsługa niepowodzenia zadania

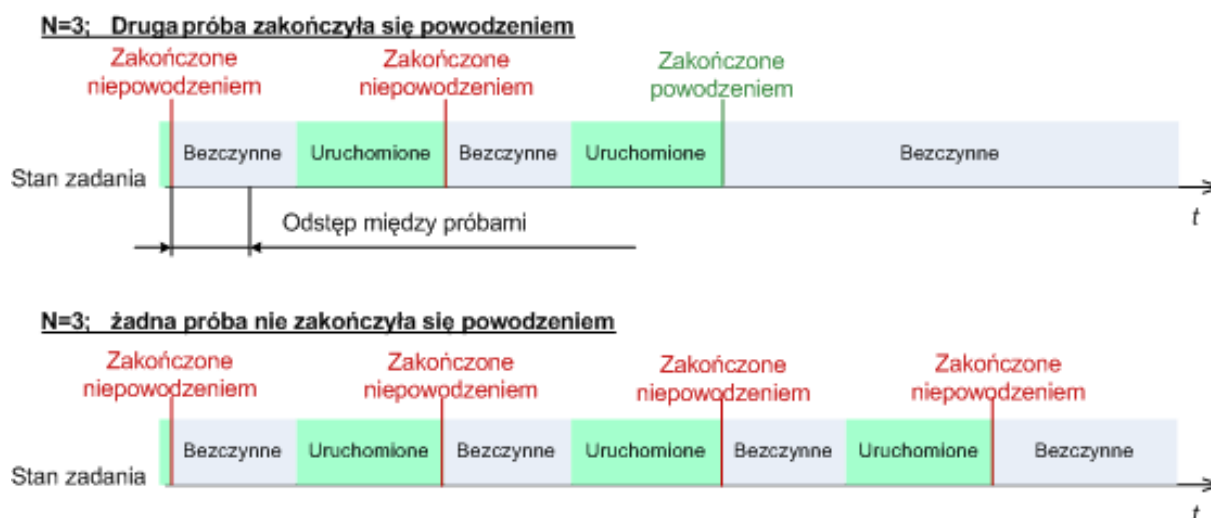
Ta opcja jest dostępna w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Opcja określa zachowanie programu, gdy nie powiedzie się wykonanie dowolnego zadania z planu tworzenia kopii zapasowych.

Ustawieniem wstępnym jest **brak ponownego uruchamiania zadania zakończonego niepowodzeniem**.

Program ponowi próbę wykonania zadania zakończonego niepowodzeniem, jeśli zostało zaznaczone pole wyboru **Ponownie uruchom zadanie zakończone niepowodzeniem** oraz została określona liczba prób i odstęp czasowy między nimi. Program wstrzyma próby, gdy jedna z nich zakończy się powodzeniem LUB po wykonaniu określonej liczby prób, w zależności od tego, który z tych warunków zostanie spełniony wcześniej.



Jeśli zadanie zakończy się niepowodzeniem z powodu błędu w planie tworzenia kopii zapasowych, można zmodyfikować plan, jeśli zadanie jest w stanie bezczynności. Jeśli zadanie jest uruchomione, należy je zatrzymać, a następnie przystąpić do modyfikacji planu tworzenia kopii zapasowych.

4.7.24 Warunki uruchomienia zadania

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa działanie programu tuż przed uruchomieniem zadania tworzenia kopii zapasowej (zbliża się zaplanowany termin lub występuje zdarzenie określone w harmonogramie), kiedy warunek (lub jeden z wielu warunków) nie został spełniony. Więcej informacji na temat warunków można znaleźć w częściach Planowanie (s. 74) i Warunki (s. 87).

Ustawienie wstępne: **Poczekaj na spełnienie warunków.**

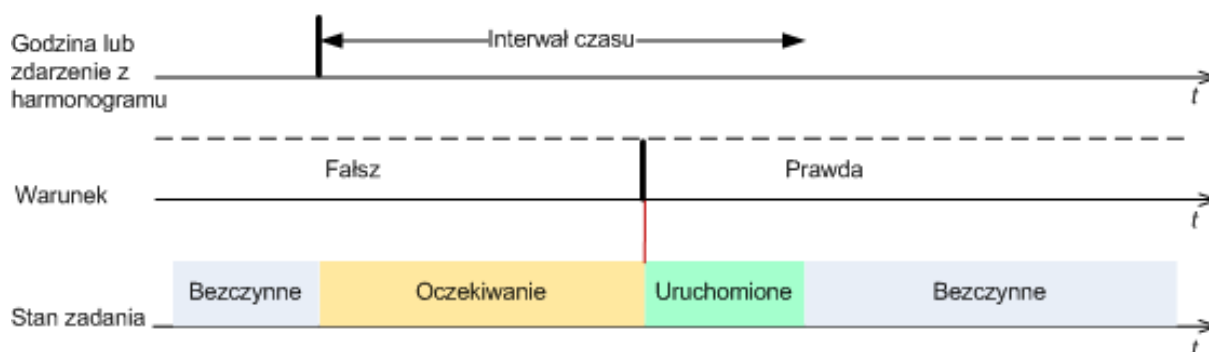
Poczekaj na spełnienie warunków

Przy tym ustawieniu funkcja harmonogramu spowoduje rozpoczęcie monitorowania warunków i uruchomienie zadania, kiedy tylko warunki zostaną spełnione. Jeżeli warunki nie zostaną w ogóle spełnione, zadanie nie zostanie uruchomione.

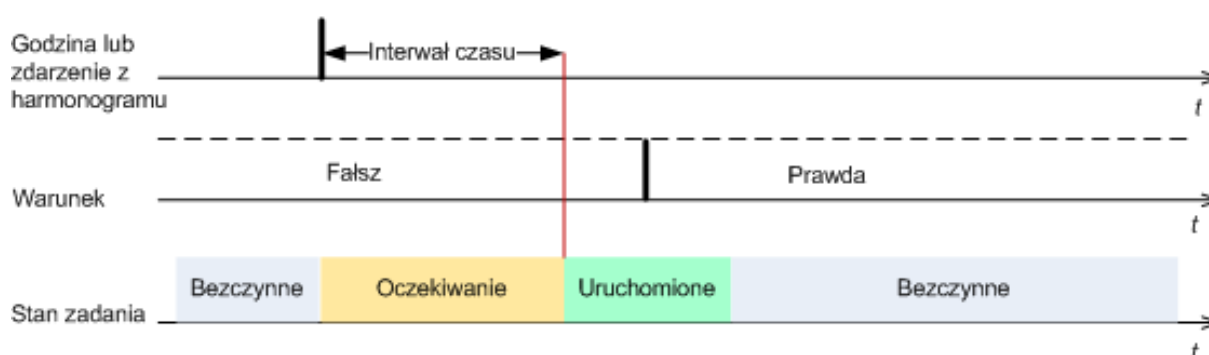
Jeśli warunki nie są spełnione przez dłuższy czas, a dalsze opóźnianie utworzenia kopii zapasowej jest ryzykowne, można wyznaczyć okres czasu, po upływie którego zadanie zostanie uruchomione niezależnie od spełnienia warunku. Zaznacz pole wyboru **Uruchom zadanie mimo to po upływie** i określ czas. Zadanie zostanie uruchomione, kiedy tylko warunki zostaną spełnione LUB maksymalny czas opóźnienia upłynie, w zależności od tego, który warunek zostanie spełniony wcześniej.

Wykres czasu: Poczekaj na spełnienie warunków

Interwał czasu > oczekiwanie na warunek



Interwał czasu < oczekiwanie na warunek



Pomiń wykonywanie zadania

Opóźnianie tworzenia kopii zapasowej jest niedopuszczalne na przykład wówczas, gdy istnieje konieczność utworzenia kopii zapasowej dokładnie o określonej godzinie. Wówczas sensowne jest pominięcie tworzenia kopii zapasowej, a nie czekanie na spełnienie warunków, szczególnie jeżeli zdarzenia następują relatywnie często.

4.7.25 Usługa kopiowania woluminów w tle

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Określa ona, czy dostawca Usługi kopiowania woluminów w tle (VSS) ma powiadamiać aplikacje obsługujące technologię VSS o planowanym rozpoczęciu tworzenia kopii zapasowej. Umożliwia to zapewnienie spójnego stanu wszystkich danych używanych przez aplikacje, a zwłaszcza dokończenie wszystkich transakcji baz danych w momencie utworzenia migawki przez program Acronis Backup & Recovery 11. Spójność danych zapewnia z kolei możliwość odzyskania aplikacji w prawidłowym stanie i umożliwia rozpoczęcie jej używania natychmiast po odzyskaniu.

Ustawienie wstępne: **Użyj Usługi kopiowania woluminów w tle (VSS).**

Używanie usługi kopiowania woluminów w tle

W przypadku zaznaczenia opcji **Użyj Usługi kopiowania woluminów w tle (VSS)** wybierz z listy dostawcę migawek:

- **Sprzętowy/programowy — wybór automatyczny** (domyślnie zaznaczone)

Usługa VSS użyje dostawcy sprzętowego obsługującego wolumin źródłowy. Jeśli usługa VSS nie znajdzie takiego dostawcy, użyje Dostawcy kopiowania w tle oprogramowania firmy Microsoft.

- **Programowy — wybór automatyczny**

W większości przypadków usługa VSS użyje Dostawcy kopiowania w tle oprogramowania firmy Microsoft.

- **Programowy — dostawca usługi VSS Acronis**

Usługa VSS użyje do wykonania migawek dostawcy VSS Acronis.

- **Programowy — dostawca systemowy**

Usługa VSS użyje do wykonania migawek dostawcy systemowego (Dostawca kopiowania w tle oprogramowania firmy Microsoft).

- **Programowy — dostawca programowy**

Usługa VSS użyje dowolnego dostępnego dostawcy programowego obsługującego wolumin źródłowy.

- **Sprzętowy — wybór automatyczny**

Usługa VSS użyje dostawcy sprzętowego obsługującego wolumin źródłowy. Jeśli nie zostanie znaleziony żaden dostawca sprzętowy, migawki będą tworzone za pomocą programu Acronis Backup & Recovery 11.

Nie używaj Usługi kopiowania woluminów w tle (VSS)

W przypadku wybrania opcji **Nie używaj usługi kopiowania woluminów w tle (VSS)** migawka danych zostanie wykonana za pomocą programu Acronis Backup & Recovery 11.

Jeśli baza danych jest niekompatybilna z Usługą VSS, wybierz **Nie używaj Usługi kopiowania woluminów w tle (VSS)**. Proces tworzenia kopii zapasowej będzie najszybszy, ale nie można zagwarantować spójności danych aplikacji, których transakcje nie zostały zakończone do czasu wykonania migawki. Za pomocą opcji Polecenia poprzedzające rejestrowanie danych/następujące po nim (s. 121) można wskazać polecenia, które powinny zostać wykonane przed wykonaniem migawki i po jej wykonaniu. Gwarantuje to spójny stan danych zapisywanych w kopii zapasowej. Można na przykład określić polecenia poprzedzające rejestrowanie danych, które spowodują wstrzymanie działania bazy danych i wyczyszczenie pamięci podręcznej w celu dokończenia wszystkich transakcji, a także polecenia po rejestrowaniu danych, które spowodują wznowienie działania bazy danych po utworzeniu migawki.

Programy zapisujące usługi kopiowania woluminów w tle

Przed utworzeniem kopii zapasowej danych aplikacji obsługujących usługę VSS należy upewnić się, że są włączone programy zapisujące usługi kopiowania woluminów w tle, sprawdzając listę programów zapisujących w systemie operacyjnym. Aby wyświetlić tę listę, należy wykonać następujące polecenie:

```
vssadmin list writers
```

Uwaga: W systemie Microsoft Windows Small Business Server 2003 moduł zapisujący programu Microsoft Exchange Server 2003 jest domyślnie wyłączony. Instrukcje dotyczące jego włączania znajdują się w odpowiednim artykule Pomocy i obsługi technicznej firmy Microsoft <http://support.microsoft.com/kb/838183/pl>.

5 Odzyskiwanie

W przypadku odzyskiwania danych należy najpierw rozważyć metodę najbardziej funkcjonalną: podłączenie konsoli do **komputera zarządzanego działającego pod kontrolą systemu operacyjnego** i utworzenie zadania odzyskiwania.

Jeśli na komputerze **system operacyjny nie uruchomi się** lub konieczne będzie odzyskanie danych **na komputer bez systemu operacyjnego**, uruchom komputer z nośnika startowego (s. 381) lub przy użyciu programu Acronis Startup Recovery Manager i skonfiguruj odzyskiwanie.

Narzędzie Acronis Universal Restore umożliwia odzyskiwanie danych i uruchamianie systemów operacyjnych **na komputerze o innej konfiguracji sprzętowej** lub na maszynie wirtualnej.

Program Acronis Backup & Recovery 11 umożliwia przesyłanie systemów operacyjnych Windows między sprzętem opartym na systemie BIOS i sprzętem obsługującym system Unified Extensible Firmware Interface (UEFI). Aby uzyskać więcej informacji, zobacz sekcję „Odzyskiwanie dysków i woluminów z systemów operacyjnych z systemem BIOS na systemy z systemem UEFI i na odwrót” (s. 149).

System Windows może zostać uruchomiony w ciągu kilku sekund — jeszcze podczas jego odzyskiwania. Korzystając z własnej technologii Acronis Active Restore (s. 156), program Acronis Backup & Recovery 11 uruchamia na komputerze system operacyjny znaleziony w kopii zapasowej, tak jakby system znajdował się na dysku fizycznym. System działa i udostępnia niezbędne usługi. W ten sposób czas przestoju systemu jest minimalny.

Wolumin dynamiczny można odzyskać na istniejący wolumin, nieprzydzielone miejsce grupy dysków lub nieprzydzielone miejsce dysku standardowego. Więcej informacji na temat odzyskiwania woluminów dynamicznych znajduje się w sekcji „Tworzenie kopii zapasowych i odzyskiwanie woluminów dynamicznych (system Windows)” (s. 36).

Aby uzyskać więcej informacji na temat sprzętowych urządzeń RAID w systemie Linux i woluminów utworzonych przez menedżera woluminów logicznych (LVM), zobacz „Odzyskiwanie urządzeń MD i woluminów logicznych” (s. 41).

Komponent Acronis Backup & Recovery 11 Agent for Windows umożliwia odzyskanie kopii zapasowej dysku (woluminu) na nową maszynę wirtualną dowolnego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) lub Red Hat Kernel-based Virtual Machine (KVM). Urządzenie wirtualne można następnie zaimportować na serwer XenServer. Pliki maszyny wirtualnej Kernel-based Virtual Machine można przenieść na komputer z systemem Linux. Następnie można uruchomić na nim maszynę wirtualną za pomocą programu Virtual Machine Manager. Stację roboczą VMware można przekonwertować na otwarty format wirtualizacji (ang. open virtualization format, OVF) przy użyciu narzędzia VMware OVF. Komponent Acronis Backup & Recovery 11 Agent for Hyper-V lub Agent for ESX(i) umożliwia utworzenie nowej maszyny wirtualnej na odpowiednim serwerze wirtualizacji.

Przed odzyskaniem danych może być konieczne przygotowanie dysków docelowych. Program Acronis Backup & Recovery 11 ma wygodne narzędzie do zarządzania dyskami, które umożliwia tworzenie lub usuwanie woluminów, zmianę stylu partycjonowania dysku, tworzenie grupy dysków lub wykonywanie innych operacji zarządzania dyskiem na docelowej konfiguracji sprzętowej, zarówno z poziomu systemu operacyjnego, jak i po awarii. Aby uzyskać więcej informacji na temat narzędzia Acronis Disk Director LV, zobacz „Zarządzanie dyskami” (s. 264).

5.1 Tworzenie zadania odzyskiwania

Aby utworzyć zadanie odzyskiwania, wykonaj poniższe czynności

Elementy do odzyskania

Wybór danych (s. 131)

Wybierz dane do odzyskania.

Poświadczenia dostępu (s. 135)

[Opcjonalnie] Podaj poświadczenia dla lokalizacji archiwum, jeśli konto zadania nie ma praw dostępu do tej lokalizacji. Aby uzyskać dostęp do tej opcji, kliknij **Pokaż poświadczenia dostępu**.

Lokalizacja odzyskiwania

Ta sekcja pojawia się po wybraniu wymaganej kopii zapasowej i zdefiniowaniu typu danych do odzyskania. Parametry określone tutaj zależą od typu odzyskiwanych danych.

Dyski (s. 136)

Woluminy (s. 139)

Pliki (s. 143)

Acronis Active Restore

[Opcjonalnie] Pole wyboru **Acronis Active Restore** jest dostępne w przypadku odzyskiwania systemu Windows począwszy od wersji Windows 2000. Funkcja Acronis Active Restore przywraca dostępność systemu niezwłocznie po rozpoczęciu jego odzyskiwania. System operacyjny uruchamia się z obrazu kopii zapasowej, a komputer działa i udostępnia niezbędne usługi. Najwyższy priorytet odzyskiwania mają dane umożliwiające obsługę żądań przychodzących. Reszta danych jest odzyskiwana w tle.

Aby uzyskać szczegółowe informacje, zobacz „Acronis Active Restore” (s. 156).

Poświadczenia dostępu (s. 136)

[Opcjonalnie] Określ poświadczenia dla miejsca docelowego, jeśli poświadczenia zadania nie umożliwiają odzyskania wybranych danych. Aby uzyskać dostęp do tego ustawienia, kliknij **Pokaż poświadczenia dostępu**.

Czas odzyskiwania

Odzyskiwanie (s. 144)

Wybierz czas rozpoczęcia odzyskiwania. Zadanie można uruchomić natychmiast po utworzeniu, zaplanować jego uruchomienie w określonym dniu i o określonej godzinie lub zapisać w celu uruchomienia ręcznego.

Parametry zadania

Nazwa zadania

[Opcjonalnie] Wprowadź unikatową nazwę zadania odzyskiwania. Dobrze dobrana nazwa umożliwi szybką identyfikację zadania spośród innych zadań.

Opcje odzyskiwania

[Opcjonalnie] Dostosuj operację odzyskiwania, konfigurując opcje, takie jak polecenia poprzedzające odzyskiwanie i następujące po nim, priorytet odzyskiwania, obsługa błędów lub opcje powiadomień. Jeśli w tej sekcji nie wykonasz żadnej czynności, zostaną użyte wartości domyślne (s. 165).

Po zmianie dowolnego z ustawień na wartość różną od domyślnej pojawi się nowy wiersz zawierający nowo skonfigurowaną wartość. Status ustawienia zmieni się z wartości

Domyślne na **Niestandardowe**. W razie ponownej zmiany ustawienia w wierszu pojawi się nowa wartość, o ile nie będzie to wartość domyślna. W przypadku wartości domyślnej wiersz zniknie. Dlatego w tej sekcji wyświetlane są tylko ustawienia różne od domyślnych.

Kliknięcie **Przywróć domyślne** powoduje przywrócenie wartości domyślnych wszystkich ustawień.

Poświadczenia zadania

[Opcjonalnie] Zadanie będzie uruchamiane z poświadczeniami użytkownika, który je utworzył. W razie konieczności można zmienić poświadczenia konta zadania. Aby uzyskać dostęp do tego ustawienia, kliknij **Pokaż poświadczenia zadania**.

[Opcjonalnie] Universal Restore for Windows/Linux

Dotyczy: odzyskiwania dysku lub woluminu systemowego. Użycie funkcji Acronis Universal Restore wymaga osobnej licencji.

Universal Restore for Windows/Linux (s. 146)

Narzędzia Acronis Universal Restore należy użyć, gdy konieczne jest odzyskanie i uruchomienie systemów operacyjnych na komputerach o innej konfiguracji sprzętowej.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby zatwierdzić utworzenie zadania odzyskiwania.

5.1.1 Elementy do odzyskania

1. Określanie lokalizacji archiwum

Określ ścieżkę archiwum w polu **Ścieżka danych** lub kliknij **Przeglądaj** i wybierz wymaganą lokalizację zgodnie z opisem w sekcji „Wybór lokalizacji archiwum” (s. 132).

Zaawansowane wersje programu Acronis Backup & Recovery 11 umożliwiają wybranie opcji określenia ścieżki archiwum jak w powyższym opisie lub skorzystanie z centralnego wykazu danych.

2. Zaznaczanie danych

Dane w kopiach zapasowych można zaznaczać na karcie **Widok danych** lub **Widok archiwum**. Na karcie **Widok danych** znajdują się wszystkie dane uwzględnione w kopiach zapasowych w ramach wybranej lokalizacji archiwum uporządkowane według wersji (daty i godziny utworzenia kopii). Na karcie **Widok archiwum** dane uwzględnione w kopiach zapasowych są uporządkowane według archiwów.

Uwaga: Odzyskiwanie na poziomie pliku za pomocą komponentu Agent for ESX(i) lub Agent for Hyper-V nie jest możliwe.

Zaznaczanie danych na karcie Widok danych

Ponieważ karta **Widok danych** ma te same funkcje co wykaz danych, zaznaczanie danych na karcie **Widok danych** i w wykazie wykonuje się w ten sam sposób. Aby uzyskać więcej informacji na temat zaznaczania danych, zobacz „Wykaz danych” (s. 134).

Zaznaczanie danych na karcie Widok archiwum

1. Rozwiń żądane archiwum i wybierz jedną z pomyślnie utworzonych kopii zapasowych uporządkowanych według daty i godziny utworzenia. Umożliwi to przywrócenie danych dysku do stanu z określonego momentu.

Jeśli lista archiwów jest zbyt długa, możesz ją odfiltrować, wybierając do wyświetlenia tylko żądany typ archiwów. W tym celu na liście **Pokaż** zaznacz żądany typ archiwów.

2. Tylko w przypadku kopii zapasowych dysków lub woluminów: z listy rozwijanej w obszarze **Zawartość kopii zapasowej** wybierz typ danych do wyświetlenia:
 - **Dyski** — aby odzyskiwać całe dyski (ze wszystkimi woluminami).
 - **Woluminy** — aby odzyskiwać pojedyncze woluminy standardowe i dynamiczne.
 - **Pliki** — aby odzyskać pojedyncze pliki i foldery.
3. W sekcji **Zawartość kopii zapasowej** zaznacz pola wyboru elementów przeznaczonych do odzyskania.
4. Kliknij **OK**.

Zaznaczanie głównego rekordu startowego






W przypadku odzyskiwania woluminu systemowego główny rekord startowy dysku zaznacza się zwykle w następujących sytuacjach:







- Nie można uruchomić systemu operacyjnego.
- Dysk jest nowy i nie ma rekordu MBR.
- Odzyskiwany jest program ładujący o charakterze niestandardowym lub inny niż z systemu Windows (na przykład LILO i GRUB).
- Geometria dysku jest inna niż dysku, którego dane są przechowywane w kopii zapasowej.

Prawdopodobnie konieczność odzyskania rekordu MBR wystąpi również przy innej okazji, ale sytuacja powyżej jest najczęstsza.

Odzyskując rekord MBR jednego dysku na inny, program Acronis Backup & Recovery 11 odzyskuje ścieżkę 0, co nie wpływa na tabelę ani układ partycji dysku docelowego. Po zakończeniu odzyskiwania program Acronis Backup & Recovery 11 automatycznie aktualizuje programy ładujące systemu Windows, więc nie ma potrzeby odzyskiwania rekordu MBR ani ścieżki 0 w systemach Windows, chyba że rekord MBR został uszkodzony.

Wybór lokalizacji archiwum

Lokalizacja	Szczegóły
 Magazyn kopii zapasowych online	Jeśli archiwum znajduje się w magazynie Acronis Online Backup Storage, kliknij Zaloguj i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę Magazyn kopii zapasowych online i wybierz konto. <i>W przypadku kopii zapasowych zapisanych w magazynie Acronis Online Backup Storage nie są obsługiwane operacje eksportowania i montowania.</i>
 Osobisty	Jeśli archiwum znajduje się w skarbcu osobistym, rozwiń grupę Osobiste i kliknij wymagany skarbiec.
 Centralny	Jeśli archiwum znajduje się w skarbcu centralnym, rozwiń grupę Centralne i kliknij odpowiedni skarbiec.
 Nazwa komputera	To jest nazwa komputera lokalnego
 Foldery lokalne	Jeśli archiwum znajduje się w folderze lokalnym na komputerze, rozwiń grupę <Nazwa komputera> i wybierz odpowiedni folder.

Lokalizacja	Szczegóły
 CD, DVD itp.	Jeśli archiwum znajduje się na nośniku optycznym, takim jak CD lub DVD, rozwiń grupę <Nazwa komputera> i wybierz żądany napęd. Najpierw włóż ostatnią płytę DVD. Następnie zgodnie z wyświetlanymi monitami wkładaj kolejno pozostałe płyty, zaczynając od pierwszej.
 Urządzenie taśmowe	Jeśli archiwum znajduje się na podłączonym lokalnie urządzeniu taśmowym, rozwiń grupę Napędy taśmowe i kliknij odpowiednie urządzenie. W autonomicznych wersjach programu Acronis Backup & Recovery 11 urządzenia taśmowe są dostępne tylko w przypadku aktualizacji z wersji Acronis Backup & Recovery 10. Aby uzyskać więcej informacji na temat używania taśm, zobacz sekcję „Urządzenia taśmowe” (s. 191).
 Foldery sieciowe	Jeśli archiwum znajduje się w udziale sieciowym, rozwiń grupę Foldery sieciowe , wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit. <i>Uwaga dla użytkowników systemu Linux: Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.</i>
 FTP, SFTP	Jeśli archiwum znajduje się na serwerze FTP lub SFTP , w polu Ścieżka wpisz nazwę lub adres serwera w następujący sposób: ftp://serwer_ftp:numer_portu lub sftp://serwer_sftp:numer_portu Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22. Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder na serwerze. Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję Użyj dostępu anonimowego . <i>Zgodnie z oryginalną specyfikacją protokołu FTP poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako zwykły tekst. Oznacza to, że nazwę użytkownika i hasło można przechwycić przy użyciu programu do przechwytywania pakietów.</i>
 Węzły magazynowania	Pracując w systemie operacyjnym, uzyskaj dostęp do węzła magazynowania przez wybór odpowiedniego skarbca centralnego. W przypadku pracy na komputerze uruchamianym z nośnika startowego: <ul style="list-style-type: none"> Aby uzyskać dostęp do skarbca zarządzanego, w polu Ścieżka wpisz następujący ciąg: bsp://adres_węzła/nazwa_skarbca/ Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.
 Dyski NFS	Jeśli archiwum jest przechowywane w udziale NFS, rozwiń grupę Dyski NFS i kliknij folder. Możliwość ta jest dostępna tylko w systemie Linux i po uruchomieniu komputera za pomocą nośnika startowego opartego na systemie Linux.

Wykaz danych

Wykaz danych ułatwia znalezienie wymaganej wersji danych i wybranie ich do odzyskania. Na komputerze zarządzanym z funkcji wykazu danych można korzystać za pomocą karty **Widok danych** odpowiadającej każdemu skarbcowi dostępnemu z tego komputera. Na serwerze zarządzania z funkcji wykazu danych można korzystać za pomocą karty **Widok danych** oraz scentralizowanego **Wykazu danych**. Scentralizowany wykaz danych przedstawia w jednym miejscu wszystkie dane przechowywane w centralnych skarbcach zarządzanych.

Wybór danych do odzyskania z kopii zapasowej

- Wykonaj jedną z następujących czynności:
 - Aby uzyskać dostęp do karty **Widok danych**, podłącz konsolę do komputera lub serwera zarządzania, przejdź do widoku **Skarbcze**, a następnie kliknij żądany skarbiec.
 - Aby uzyskać dostęp do **Wykazu danych**, podłącz konsolę do serwera zarządzania i w drzewie **Nawigacja** wybierz **Wykaz danych**.
- W polu **Pokaż** określ typ danych do wyświetlenia:
 - Wybierz **Komputery/dyski/woluminy**, aby przeglądać i wyszukiwać całe dyski i woluminy w kopiach zapasowych na poziomie dysku.
 - Wybierz **Foldery/pliki**, aby przeglądać i wyszukiwać pliki i foldery w kopiach zapasowych zarówno na poziomie pliku, jak i na poziomie dysku.
- W polu **Wyświetl dane uwzględnione w kopii zapasowej dla** wskaż okres, dla którego mają być wyświetlane dane z kopii zapasowej.
- Wykonaj jedną z następujących czynności:
 - Wybierz dane przeznaczone do odzyskania w drzewie wykazu lub w tabeli znajdującej się po jego prawej stronie.
 - W ciągu wyszukiwania wpisz informacje pomocne w identyfikacji wymaganych elementów danych (na przykład nazwę komputera, pliku lub folderu bądź etykietę dysku), a następnie kliknij **Szukaj**. Można korzystać z symboli wieloznacznych gwiazdki (*) i znaku zapytania (?).
W wyniku tej operacji okno **Szukaj** będzie zawierać listę elementów danych kopii zapasowych, których nazwy całkowicie lub częściowo pokrywają się z wprowadzoną wartością. Jeśli lista znalezionych elementów jest zbyt długa, zawęż kryteria wyszukiwania, określając zakres dat lub godzin utworzenia kopii zapasowych oraz zakres rozmiaru elementów umieszczonych w kopiach. Po znalezieniu szukanych danych zaznacz je i kliknij **OK**, aby powrócić do **Wykazu danych/Widoku danych**.
- Za pomocą listy **Wersje** wybierz czas, do którego chcesz przywrócić dane. Domyślnie dane są przywracane do ostatniego dostępnego momentu w okresie wybranym w kroku 3.
- Po wybraniu wymaganych danych kliknij **Odzyskaj** i skonfiguruj parametry operacji odzyskiwania.

Co zrobić w przypadku braku danych w wykazie lub widoku danych

Możliwe są następujące przyczyny takiego stanu rzeczy:

Nieprawidłowy ustawiony okres

Poszukiwane dane nie zostały zapisane w kopii zapasowej w okresie ustawionym w polu **Wyświetl dane uwzględnione w kopii zapasowej dla**.

Rozwiązanie: Wydłuż okres i spróbuj ponownie.

Katalogowanie jest wyłączone

Jeśli wyświetlono jedynie część poszukiwanych danych lub nie wyświetlono ich wcale, najprawdopodobniej w trakcie wykonywania kopii zapasowych opcja katalogowania kopii zapasowych (s. 108) była wyłączona.

Rozwiązania:

- Uruchom katalogowanie ręcznie, klikając **Rozpocznij katalogowanie**. W przypadku **Wykazu danych** zostaną skatalogowane wszystkie kopie zapasowe przechowywane w skarbcach zarządzanych. W przypadku **Widoku danych** zostaną skatalogowane jedynie kopie zapasowe przechowywane w wybranym skarbcu. Operacja katalogowania nie obejmie kopii zapasowych, które zostały już skatalogowane wcześniej.
- Ponieważ operacja katalogowania dużej liczby danych w kopiach zapasowych może zająć dużo czasu, lepszym rozwiązaniem może być użycie **Widoku archiwum** odpowiedniego skarbcza. Aby uzyskać więcej informacji na temat Widoku archiwum, zobacz „Przeglądanie zawartości skarbcza i wybór danych” w sekcji Korzystanie ze skarbców (s. 176).

Dane nie są obsługiwane przez wykaz

Następujące typy danych nie mogą być wyświetlane w wykazie ani widoku danych:

- Dane z zaszyfrowanych i chronionych hasłem archiwów.
- Dane zapisane w kopiach zapasowych na nośnikach wymiennych, takich jak płyty CD, DVD, BD lub kasety Iomega REV.
- Dane zapisane w kopiach zapasowych w magazynie Acronis Online Backup Storage.
- Dane zapisane w kopiach zapasowych przy użyciu programu Acronis True Image Echo lub w starszych wersjach programu.
- Dane zapisane przy użyciu uproszczonego nazewnictwa kopii zapasowych.

Rozwiązanie: Do przeglądania takich danych służy karta **Widok archiwum** odpowiedniego skarbcza.

Dane nie są zawarte w scentralizowanym katalogu

Dane ze skarbców osobistych (s. 185) nie są wyświetlane w scentralizowanym katalogu.

Rozwiązanie: Aby móc przeglądać takie dane, połącz się bezpośrednio z komputerem, wybierz żądany skarbiec osobisty i kliknij **Widok danych**.

5.1.2 Poświadczenia dostępu do lokalizacji

Określ poświadczenia wymagane w celu uzyskania dostępu do lokalizacji, w której znajduje się kopia zapasowa.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń zadania**
Program uzyska dostęp do lokalizacji za pomocą poświadczeń konta zadania określonego w sekcji **Parametry zadania**.
- **Użyj następujących poświadczeń**
Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Użyj tej opcji, jeśli konto zadania nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbcza węzła magazynowania.
Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejść przy użyciu programu do przechwytywania pakietów.

5.1.3 Poświadczenia dostępu do miejsca docelowego

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń zadania**

Program uzyska dostęp do miejsca docelowego za pomocą poświadczeń konta zadania określonego w sekcji **Parametry zadania**.

- **Użyj następujących poświadczeń**

Program uzyska dostęp do miejsca docelowego przy użyciu określonych poświadczeń. Użyj tej opcji, jeśli konto zadania nie ma uprawnień dostępu do miejsca docelowego.

Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

5.1.4 Lokalizacja odzyskiwania

Określ miejsce docelowe odzyskiwania wybranych danych.

Wybór dysków docelowych

Dostępne dyski docelowe zależą od agentów uruchomionych na komputerze.

Odzyskaj do:

Komputer fizyczny

Opcja dostępna, gdy jest zainstalowany komponent Acronis Backup & Recovery 11 Agent for Windows lub Agent for Linux.

Wybrane dyski zostaną odzyskane na dyski fizyczne komputera, do którego jest podłączona konsola. Po wybraniu tej opcji należy wykonać standardową procedurę mapowania dysków opisaną poniżej.

Nowa maszyna wirtualna

- *Jeśli jest zainstalowany komponent Acronis Backup & Recovery 11 Agent for Windows.*

Wybrane dyski zostaną odzyskane na nową maszynę wirtualną jednego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation lub Citrix XenServer Open Virtual Appliance (OVA). Pliki maszyny wirtualnej zostaną zapisane w określonym miejscu docelowym.

- *Jeśli jest zainstalowany komponent Acronis Backup & Recovery 11 Agent for Hyper-V lub Agent for ESX(i).*

Są to agenty umożliwiające utworzenie nowej maszyny wirtualnej na określonym serwerze wirtualizacji.

Nowa maszyna wirtualna zostanie skonfigurowana automatycznie — w miarę możliwości zostaną skopiowane ustawienia konfiguracji maszyny źródłowej. Konfiguracja zostanie wyświetlona w sekcji **Ustawienia maszyn wirtualnych** (s. 160). Sprawdź te ustawienia i w razie potrzeby wprowadź w nich zmiany.

Następnie wykonaj standardową procedurę mapowania dysków opisaną poniżej.

Istniejąca maszyna wirtualna

Opcja dostępna, gdy jest zainstalowany komponent Acronis Backup & Recovery 11 Agent lub Hyper-V lub Agent for ESX(i).

Wybierając tę opcję, należy określić serwer wirtualizacji i docelową maszynę wirtualną. Następnie wykonaj standardową procedurę mapowania dysków opisaną poniżej.

Należy pamiętać, że przed rozpoczęciem odzyskiwania maszyna docelowa zostanie automatycznie wyłączona. Aby wyłączyć ją ręcznie, należy zmienić ustawienie opcji Zarządzanie zasilaniem maszyn wirtualnych.

Dyski/woluminy

Mapuj automatycznie

Program Acronis Backup & Recovery 11 próbuje zamapować wybrane dyski na dyski docelowe zgodnie z opisem w sekcji „Na jakiej zasadzie funkcjonuje mapowanie automatyczne” (s. 138). Jeśli wyniki mapowania nie są zadowalające, zamapuj dyski ręcznie. W tym celu należy usunąć mapowanie dysków w odwrotnej kolejności, tj. w pierwszej kolejności trzeba usunąć mapowanie dysku zamapowanego jako ostatni. Następnie należy zamapować dyski ręcznie zgodnie z poniższą procedurą.

Nr dysku:

Nr dysku (MODEL) (s. 137)

Wybierz dysk docelowy dla każdego z dysków źródłowych.

Podpis NT (s. 137)

Wybierz sposób obsługi podpisu odzyskanego dysku. Podpis dysku jest używany w systemie Windows i jądrach systemu Linux w wersji 2.6 lub nowszej.

Dysk docelowy

Aby określić dysk docelowy:

1. Wybierz dysk, na który chcesz odzyskać wybrany dysk. Rozmiar dysku docelowego powinien być co najmniej taki sam, jak rozmiar nieskompresowanych danych w obrazie.
2. Kliknij **OK**.

Wszystkie dane przechowywane na dysku docelowym zostaną zastąpione danymi z kopii zapasowej, dlatego należy zachować ostrożność i uważać, aby nie utracić potrzebnych danych, których nie ma w kopii zapasowej.

Podpis NT

Podpis NT to rekord przechowywany w głównym rekordzie startowym (MBR). Umożliwia on unikatową identyfikację dysku w systemie operacyjnym.

Podczas odzyskiwania dysku zawierającego wolumin systemowy można wybrać sposób postępowania z podpisem NT dysku docelowego. Określ dowolne z następujących parametrów:

- **Wybierz automatycznie**

Program zachowa podpis NT dysku docelowego, jeśli jest on taki sam jak podpis NT przechowywany w kopii zapasowej. (Innymi słowy — odzyskiwanie na ten sam dysk, który był uwzględniony w kopii zapasowej.) W innym razie program wygeneruje nowy podpis NT dla dysku docelowego.

Jest to domyślny wybór, zalecany w większości przypadków. Z podanych niżej ustawień należy korzystać jedynie w razie konieczności.

- **Utwórz nowy**

Program Acronis Backup & Recovery 11 utworzy nowy podpis NT docelowego dysku twardego.

- **Odzyskaj z kopii zapasowej**

Produkt Acronis Backup & Recovery 11 zmieni podpis NT docelowego dysku twardego na podpis z kopii zapasowej dysku.

Uwaga: Należy koniecznie upewnić się, że żaden z zamontowanych w komputerze dysków nie ma tej samej sygnatury NT. W przeciwnym razie system operacyjny uruchomi się z pierwszego dysku, a po wykryciu identycznego podpisu drugiego dysku automatycznie wygeneruje nowy unikatowy podpis NT i przypisze go drugiemu dyskowi. Skutkiem tego wszystkie woluminy na drugim dysku tracą swoje litery, wszystkie ścieżki na dysku stają się nieprawidłowe, a programy nie mogą znaleźć swoich plików. Uruchomienie systemu operacyjnego umieszczonego na tym dysku jest niemożliwe.

Odzyskanie podpisu dysku może być pożądane z następujących przyczyn:

- Program Acronis Backup & Recovery 11 planuje zadania przy użyciu podpisu źródłowego dysku twardego. W przypadku odzyskania tego samego podpisu dysku nie trzeba ponownie tworzyć ani edytować utworzonych wcześniej zadań.
 - Niektóre z zainstalowanych aplikacji wykorzystują podpis dysku do celów licencyjnych lub innych.
 - Umożliwia to zachowanie wszystkich punktów przywracania systemu Windows na odzyskanym dysku.
 - Umożliwia odzyskanie migawek usługi kopiowania woluminów w tle używanej przez funkcję „Poprzednie wersje” w systemie Windows Vista.
- **Zachowaj istniejący**
- Program zachowa bez zmian istniejący podpis NT docelowego dysku twardego.

Na jakiej zasadzie funkcjonuje mapowanie automatyczne

Program Acronis Backup & Recovery 11 automatycznie mapuje dyski lub woluminy na dyski docelowe tylko w przypadku zachowania możliwości uruchamiania systemu. W innym razie mapowanie automatyczne jest anulowane i należy ręcznie zamapować dyski lub woluminy.

Konieczność ręcznego mapowania woluminów dotyczy również woluminów logicznych systemu Linux oraz programowych macierzy RAID systemu Linux (urządzeń MD). Aby uzyskać więcej informacji na temat odzyskiwania woluminów logicznych i urządzeń MD, zobacz Odzyskiwanie urządzeń MD i woluminów logicznych (s. 41).

Mapowanie automatyczne odbywa się w opisany poniżej sposób.

1. Jeśli dysk lub wolumin jest odzyskiwany do oryginalnej lokalizacji, proces mapowania odtwarza układ oryginalnego dysku/woluminu.

Oryginalna lokalizacja dysku lub woluminu oznacza dokładnie ten sam dysk lub wolumin, który był uwzględniony w kopii zapasowej. Wolumin nie zostanie uznany za oryginalny, jeśli jego rozmiar, lokalizacja bądź inne parametry fizyczne będą inne niż w zapisanej kopii zapasowej. Zmiana litery lub etykiety woluminu nie utrudnia programowi jego rozpoznania.

2. Jeśli dysk lub wolumin jest odzyskiwany do innej lokalizacji:

- **Podczas odzyskiwania dysków:** program sprawdza rozmiary i woluminy dysków docelowych. Dysk docelowy nie może zawierać żadnych woluminów, a jego rozmiar musi być dostatecznie duży, aby pomieścić odzyskiwany dysk. Niezainicjowane dyski docelowe zostaną automatycznie zainicjowane.

Jeśli nie można znaleźć wymaganych dysków, należy je ręcznie zamapować.

- **Podczas odzyskiwania woluminów:** program sprawdza wielkość nieprzydzielonego miejsca na dyskach docelowych.

Jeśli ilość nieprzydzielonego miejsca będzie wystarczająca, woluminy zostaną odzyskane „bez zmian”.

Jeśli ilość nieprzydzielonego miejsca na dyskach docelowych będzie mniejsza niż rozmiar odzyskiwanych woluminów, woluminy zostaną proporcjonalnie pomniejszone (przez zmniejszenie ilości wolnego miejsca), aby zmieściły się na nieprzydzielonym miejscu. Jeśli pomniejszone woluminy w dalszym ciągu nie będą się mieścić na nieprzydzielonym miejscu, trzeba będzie je ręcznie zamapować.

Wybieranie woluminów docelowych

Dostępne miejsca docelowe woluminów zależą od agentów uruchomionych na komputerze.

Odzyskaj do:

Komputer fizyczny

Opcja dostępna, gdy jest zainstalowany komponent Acronis Backup & Recovery 11 Agent for Windows lub Agent for Linux.

Wybrane woluminy zostaną odzyskane na dyski fizyczne komputera, do którego jest podłączona konsola. Po wybraniu tej opcji należy wykonać standardową procedurę mapowania dysków opisaną poniżej.

Nowa maszyna wirtualna

- *Jeśli jest zainstalowany komponent Acronis Backup & Recovery 11 Agent for Windows.*

Wybrane woluminy zostaną odzyskane na nową maszynę wirtualną jednego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation lub Citrix XenServer Open Virtual Appliance (OVA). Pliki maszyny wirtualnej zostaną zapisane w określonym miejscu docelowym.

- *Jeśli jest zainstalowany komponent Acronis Backup & Recovery 11 Agent for Hyper-V lub Agent for ESX(i).*

Są to agenty umożliwiające utworzenie nowej maszyny wirtualnej na określonym serwerze wirtualizacji.

Nowa maszyna wirtualna zostanie skonfigurowana automatycznie — w miarę możliwości zostaną skopiowane ustawienia konfiguracji maszyny źródłowej. Konfiguracja zostanie wyświetlona w sekcji **Ustawienia maszyn wirtualnych** (s. 160). Sprawdź te ustawienia i w razie potrzeby wprowadź w nich zmiany.

Następnie należy wykonać standardową procedurę mapowania woluminów opisaną poniżej.

Istniejąca maszyna wirtualna

Opcja dostępna, gdy jest zainstalowany komponent Acronis Backup & Recovery 11 Agent lub Hyper-V lub Agent for ESX(i).

Wybierając tę opcję, należy określić serwer wirtualizacji i docelową maszynę wirtualną. Następnie należy wykonać standardową procedurę mapowania woluminów opisaną poniżej.

Należy pamiętać, że przed rozpoczęciem odzyskiwania maszyna docelowa zostanie automatycznie wyłączona. Aby wyłączyć ją ręcznie, należy zmienić ustawienie opcji Zarządzanie zasilaniem maszyn wirtualnych.

Dyski/woluminy

Mapuj automatycznie

Program Acronis Backup & Recovery 11 próbuje zamapować wybrane woluminy na dyski docelowe zgodnie z opisem w sekcji „Na jakiej zasadzie funkcjonuje mapowanie automatyczne” (s. 138). Jeśli wyniki mapowania nie są zadowalające, zamapuj woluminy ręcznie. W tym celu należy usunąć mapowanie woluminów w odwrotnej kolejności, tj. w pierwszej kolejności trzeba usunąć mapowanie woluminu zamapowanego jako ostatni. Następnie należy zamapować woluminy ręcznie zgodnie z poniższą procedurą.

Odzyskaj MBR [nr dysku] na: [jeśli wybrano odzyskiwanie głównego rekordu rozruchowego]

Nr dysku (s. 140)

Wybierz dysk, na który chcesz odzyskać główny rekord rozruchowy.

Podpis NT: (s. 137)

Wybierz sposób obsługi podpisu dysku umieszczonego w głównym rekordzie rozruchowym. Podpis dysku jest używany w systemie Windows i jądrach systemu Linux w wersji 2.6 lub nowszej.

Odzyskaj [wolumin] [litera] na:

Nr dysku/Wolumin

Mapowanie kolejno wszystkich woluminów źródłowych na wolumin lub nieprzydzielone miejsce na dysku docelowym.

Rozmiar: (s. 141)

[Opcjonalnie] Zmień rozmiar, lokalizację i inne właściwości odzyskanego woluminu.

Miejsce docelowe rekordu MBR

Aby określić dysk docelowy:

1. Wybierz dysk, na który chcesz odzyskać rekord MBR.
2. Kliknij **OK**.

Miejsce docelowe woluminu

Aby określić wolumin docelowy lub nieprzydzielone miejsce

1. Wybierz wolumin lub nieprzydzielone miejsce, gdzie wybrany wolumin ma zostać odzyskany. Docelowy wolumin lub docelowe nieprzydzielone miejsce powinny mieć przynajmniej taki sam rozmiar jak obraz danych nieskompresowanych.
2. Kliknij **OK**.

Wszystkie dane przechowywane w woluminie docelowym zostaną zastąpione danymi kopii zapasowej, tak więc należy zachować ostrożność i uważać na dane, które nie mają kopii zapasowej, a mogą być potrzebne.

W przypadku korzystania z nośnika startowego

Litery dysków widoczne podczas pracy z nośnikiem startowym w stylu systemu Windows mogą różnić się od sposobu identyfikacji dysków przez system Windows. Na przykład dysk D: w narzędziu ratunkowym może odpowiadać dyskowi E: w systemie Windows.

Ostrożnie! Dla bezpieczeństwa zaleca się przypisywanie unikatowych nazw woluminów.

Na nośniku startowym w stylu systemu Linux dyski i woluminy lokalne są pokazywane jako odmontowane (sda1, sda2...).

Zmiana właściwości woluminu

Rozmiar i lokalizacja

W procesie odzyskiwania woluminu na standardowy dysk MBR można zmienić rozmiar i umiejscowienie woluminu, przeciągając go lub jego krawędzie myszą albo wprowadzając odpowiednie wartości we właściwych polach. Dzięki tej funkcji można rozłożyć miejsce na dysku między odzyskiwane woluminy. W tym przypadku trzeba najpierw odzyskać wolumin, który będzie zmniejszany.

Uwaga: Nie można zmieniać rozmiaru woluminów, których kopie zapasowe były tworzone z użyciem opcji „sektor po sektorze”.

Wskazówka: Rozmiaru woluminu nie można zmienić w przypadku jego odzyskiwania z kopii zapasowej podzielonej na kilka nośników wymiennych. Aby zmienić rozmiar woluminu, należy skopiować wszystkie części kopii zapasowej do jednej lokalizacji na dysku twardym.

Typ

Standardowy dysk MBR może zawierać maksymalnie cztery woluminy podstawowe lub maksymalnie trzy woluminy podstawowe i wiele dysków logicznych. Program domyślnie wybiera oryginalny typ woluminu. W razie potrzeby to ustawienie można zmienić.

- **Podstawowy.** Informacje dotyczące woluminów podstawowych znajdują się w tabeli partycji MBR. Większość systemów operacyjnych można uruchomić tylko z woluminu podstawowego pierwszego dysku twardego, ale liczba woluminów podstawowych jest ograniczona.
Chcąc odzyskać wolumin systemowy na standardowy dysk MBR, zaznacz pole wyboru Aktywny. Wolumin aktywny jest używany do ładowania systemu operacyjnego. Wybór opcji Aktywny w przypadku woluminu bez zainstalowanego systemu operacyjnego może uniemożliwić uruchomienie komputera. Dysku logicznego ani woluminu dynamicznego nie można ustawić jako aktywnego.
- **Logiczny.** Informacje dotyczące woluminów logicznych znajdują się nie w głównym rekordzie startowym, ale w tablicy partycji rozszerzonej. Liczba woluminów logicznych na dysku jest nieograniczona. Woluminu logicznego nie można ustawić jako aktywnego. W przypadku odzyskiwania woluminu systemowego na inny dysk twardy, który zawiera własne woluminy i system operacyjny, najczęściej potrzebne są tylko dane. W takiej sytuacji można odzyskać wolumin jako logiczny, aby uzyskać dostęp do samych danych.

System plików

Domyślnie odzyskany wolumin będzie miał ten sam system plików co wolumin oryginalny. Jeśli jest to konieczne, w trakcie odzyskiwania można zmienić system plików woluminu.

Program Acronis Backup & Recovery 11 umożliwia następujące rodzaje konwersji między systemami plików: FAT 16 -> FAT 32 oraz Ext2 -> Ext3. W przypadku woluminów z innymi macierzystymi systemami plików ta opcja jest niedostępna.

Załóżmy, że wolumin ze starego dysku o małej pojemności z systemem plików FAT16 chcemy odzyskać na nowszy dysk. System plików FAT16 nie będzie skuteczny, co więcej — jego ustawienie na dysku twardym o dużej pojemności może okazać się niemożliwe. Wynika to z faktu, że system plików FAT16 obsługuje woluminy o maksymalnej wielkości 4 GB, zatem bez zmiany systemu plików odzyskanie woluminu FAT16 o wielkości 4 GB na wolumin przekraczający ten limit jest niemożliwe. W tej sytuacji zaleca się zmianę systemu plików z FAT16 na FAT32.

Starsze systemy operacyjne (MS-DOS, Windows 95 i Windows NT 3.x, 4.x) nie obsługują systemu plików FAT32 i nie będą działały po odzyskaniu woluminu i zmianie jego systemu plików. Można je zwykle odzyskać tylko na wolumin z systemem plików FAT16.

Wyrównanie woluminów (partycji)

Program Acronis Backup & Recovery 11 automatycznie poprawia nieprawidłowo wyrównane woluminy — sytuację, w której klastry woluminów nie są wyrównane z sektorami dysku. Brak wyrównania występuje w przypadku odzyskiwania woluminów utworzonych z użyciem schematu adresowania cylinder/głowica/sektor (CHS) nadysku twardym (HDD) lub dysku Solid-State Drive (SSD) z sektorami o rozmiarze 4 KB. Schemat adresowania CHS jest na przykład stosowany we wszystkich systemach operacyjnych Windows starszych niż Windows Vista.

Jeśli woluminy są niewyrównane, klastrer nachodzi na więcej sektorów fizycznych niż w przypadku wyrównania. W związku z tym po każdej zmianie danych trzeba wymazać i ponownie zapisać więcej sektorów fizycznych. Takie nadmiarowe operacje odczytu/zapisu zauważalnie spowalniają dysk i obniżają wydajność całego systemu. Brak wyrównania w przypadku dysków SSD obniża nie tylko wydajność systemu, ale także trwałość dysku. Komórki pamięci dysku SSD są zaprojektowane z myślą o określonej ilości cykli odczytu/zapisu, dlatego nadmiarowe operacje odczytu/zapisu prowadzą do przedwczesnego zużycia dysku SSD.

W przypadku odzyskiwania woluminów dynamicznych oraz woluminów logicznych utworzonych w systemie Linux pod kontrolą menedżera woluminów logicznych (LVM) właściwe wyrównanie jest konfigurowane automatycznie.

W przypadku odzyskiwania woluminów standardowych MBR i GPT można ręcznie wybrać metodę wyrównywania, jeśli z jakiegoś powodu wyrównanie automatyczne nie jest preferowane. Dostępne są następujące opcje:

- **Wybierz automatycznie** — wartość domyślna, zalecana. Oprogramowanie automatycznie ustawi właściwy tryb wyrównywania w oparciu o właściwości dysku/woluminu źródłowego i docelowego.
Z podanych niżej opcji należy korzystać jedynie w przypadku absolutnej konieczności.
- **CHS (63 sektory)** — wybierz tę opcję, jeśli odzyskany wolumin będzie używany w systemach Microsoft Windows XP oraz Windows Server 2003 (lub starszych) na dyskach o rozmiarze sektora fizycznego równym 512 bajtów.
- **VMWare VMFS (64 KB)** — wybierz tę opcję, jeśli wolumin jest odzyskiwany jako partycja systemu plików maszyny wirtualnej VMware.
- **Wyrównanie systemu Vista (1 MB)** — wybierz tę opcję, jeśli odzyskany wolumin będzie używany w systemie operacyjnym Windows nie starszym niż Windows Vista, lub w przypadku odzyskiwania woluminów na dysk HDD lub SSD o rozmiarze sektora równym 4 KB.

- **Niestandardowe** — opcja umożliwiająca ręczne określenie wyrównania woluminu. Zaleca się, aby ta wartość była wielokrotnością rozmiaru sektora fizycznego.

Litera dysku logicznego (tylko Windows)

Domyślnie do woluminu zostanie przypisana pierwsza niewykorzystana litera. Aby przypisać inną literę, wybierz żądaną literę z listy rozwijanej.

Wybór wartości pustej oznacza brak przypisania litery do odzyskanego woluminu i ukrycie go przed systemem operacyjnym. Nie należy przypisywać liter do woluminów, które są niedostępne dla systemu Windows, takich jak woluminy inne niż FAT i NTFS.

Wybór lokalizacji docelowej plików i folderów

Lokalizacja odzyskiwania

Miejsce docelowe

Wybierz lokalizację, do której zostaną odzyskane pliki z kopii zapasowej:

- **Oryginalna lokalizacja**
Pliki i foldery zostaną odzyskane w tej samej ścieżce, w jakiej są zapisane w kopii zapasowej. Jeśli na przykład utworzono kopię zapasową wszystkich plików i folderów w ścieżce *C:\Documents\Finance\Reports*, pliki zostaną odzyskane w tej samej ścieżce. Jeśli folder nie istnieje, zostanie utworzony automatycznie.
- **Nowa lokalizacja**
Pliki zostaną odzyskane w lokalizacji określonej w drzewie. Pliki i foldery zostaną odzyskane bez odtwarzania pełnej ścieżki, chyba że pole wyboru **Odzyskaj bez pełnej ścieżki** będzie wyczyszczone.

Agent odzyskiwania

Wybierz komponent Acronis Agent, który przeprowadzi odzyskiwanie plików. Możliwość wyboru agenta jest dostępna tylko wtedy, gdy program nie może wykryć agenta na komputerze, do którego będą odzyskiwane pliki.

Zastępowanie

Określ zachowanie programu, gdy w folderze docelowym znajdzie plik o takiej samej nazwie jak w archiwum:

- **Zastąp istniejący plik** — plik znajdujący się w kopii zapasowej otrzyma pierwszeństwo przed plikiem na dysku twardym.
- **Zastąp istniejący plik, jeśli jest starszy** — pierwszeństwo otrzyma plik zmodyfikowany później, niezależnie od tego, czy znajduje się w kopii zapasowej, czy na dysku.
- **Nie zastępuj istniejącego pliku** — plik znajdujący się na dysku twardym otrzyma pierwszeństwo przed plikiem w kopii zapasowej.

Po zezwoleniu na zastępowanie plików nadal można zapobiec zastępowaniu określonych plików, wykluczając je z operacji odzyskiwania.

Wykluczenia podczas odzyskiwania (s. 143)

Określ pliki i foldery, których nie chcesz odzyskiwać.

Wykluczenia podczas odzyskiwania

Skonfiguruj wykluczenia określonych plików, których nie chcesz odzyskiwać.

Aby utworzyć listę masek plików, użyj przycisków **Dodaj**, **Edytuj**, **Usuń** i **Usuń wszystko**. Pliki, których nazwy pasują do dowolnej z masek, zostaną pominięte podczas odzyskiwania.

W masce plików można użyć jednego lub kilku symboli wieloznacznych * i ?:

- Gwiazdka (*) zastępuje dowolną liczbę znaków w nazwie pliku (w tym również zero). Na przykład maska Dok*.txt zwraca pliki takie jak Dok.txt i Dokument.txt
- Znak zapytania (?) zastępuje dokładnie jeden znak w nazwie pliku. Na przykład maska Dok?.txt zwraca pliki takie jak Dok1.txt i Doku.txt, ale nie zwraca plików Dok.txt ani Dok11.txt

Przykłady wykluczeń

Kryterium	Przykład	Opis
Windows i Linux		
Według nazwy	F.log F	Wyklucza wszystkie pliki o nazwie „F.log”. Wyklucza wszystkie foldery o nazwie „F”.
Według maski (*)	*.log F*	Wyklucza wszystkie pliki z rozszerzeniem .log. Wyklucza wszystkie pliki i foldery, których nazwa rozpoczyna się od litery „F” (np. foldery F, F1 i pliki F.log, F1.log).
Według maski (?)	F????.log	Wyklucza wszystkie pliki z rozszerzeniem .log, których nazwy składają się z czterech znaków i zaczynają od litery „F”.
Windows		
Według ścieżki pliku	Finanse\F.log	Wyklucza pliki o nazwie „F.log” z wszystkich folderów o nazwie „Finanse”.
Według ścieżki folderu	Finanse\F\ lub Finanse\F	Wyklucza foldery o nazwie „F” z wszystkich folderów o nazwie „Finanse”.
Linux		
Według ścieżki pliku	/home/user/Finanse/F.log	Wyklucza plik „F.log” znajdujący się w folderze /home/user/Finanse.

Powyższe ustawienia nie dotyczą plików lub folderów, które zostały wprost wybrane do odzyskania. Załóżmy, że wybierzesz na przykład folder MojFolder i plik MojPlik.tmp znajdujący się poza tym folderem oraz zdecydujesz o pominięciu wszystkich plików .tmp. W tej sytuacji w trakcie odzyskiwania zostaną pominięte wszystkie pliki .tmp znajdujące się w folderze MojFolder, ale plik MojPlik.tmp nie zostanie pominięty.

5.1.5 Czas odzyskiwania

Wybierz czas rozpoczęcia wykonywania zadania odzyskiwania:

- **Teraz** — zadanie odzyskiwania rozpocznie się natychmiast po kliknięciu ostatniego przycisku **OK** na stronie **Odzyskaj dane**.
- **Później** — zadanie odzyskiwania zostanie uruchomione ręcznie w późniejszym terminie. Jeśli musisz zaplanować zadanie, wyczyść pole wyboru **Zadanie zostanie uruchomione ręcznie** i określ żądaną datę i godzinę.

5.1.6 Poświadczenia zadania

Określ poświadczenia konta, na którym zadanie będzie uruchamiane.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń bieżącego użytkownika**

Zadanie będzie uruchamiane przy użyciu poświadczeń, z którymi zalogował się użytkownik rozpoczynający zadania. Jeśli zadanie ma zostać uruchomione według harmonogramu, w momencie zakończenia tworzenia zadania użytkownik zostanie poproszony o aktualne hasło użytkownika.

- **Użyj następujących poświadczeń**

Zadanie będzie zawsze uruchamiane przy użyciu poświadczeń określonych przez użytkownika, niezależnie od tego, czy zadanie będzie uruchamiane ręcznie, czy wykonywane według harmonogramu.

Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Więcej informacji na temat używania poświadczeń w programie Acronis Backup & Recovery 11 można znaleźć w sekcji Właściciele i poświadczenia (s. 32).

Aby dowiedzieć się więcej na temat operacji dostępnych w zależności od uprawnień użytkownika, zobacz sekcję Uprawnienia użytkownika na komputerze zarządzanym.

5.2 Acronis Universal Restore

Acronis Universal Restore to zastrzeżona technologia firmy Acronis, która ułatwia odzyskiwanie i uruchamianie systemu operacyjnego na sprzęcie o innej konfiguracji lub na maszynie wirtualnej. Funkcja Universal Restore niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu operacyjnego, takimi jak kontrolery pamięci, płyta główna i chipset.

Jest ona niezwykle przydatna w następujących przypadkach:

1. błyskawiczne odzyskanie uszkodzonego systemu przy użyciu innego sprzętu;
2. niezależne od sprzętu klonowanie i wdrażanie systemów operacyjnych;
3. migrację komputerów typu fizyczny na fizyczny, fizyczny na wirtualny oraz wirtualny na fizyczny.

5.2.1 Uzyskiwanie narzędzia Universal Restore

Funkcja Universal Restore jest dostępna zawsze podczas odzyskiwania systemu z magazynu online.

Moduł Universal Restore jest dostępny bezpłatnie z programami Acronis Backup & Recovery 11 Advanced Server SBS Edition oraz Virtual Edition.

W przypadku innych wersji produktów komponent ten należy nabyć oddzielnie. Jest on wyposażony we własną licencję

Aby umożliwić korzystanie z funkcji Universal Restore na komputerze zarządzanym, wykonaj jedną z następujących czynności:

- Zainstaluj komponent Universal Restore z pakietu instalacyjnego produktu (wraz z programem Agent for Windows, Agent for Linux lub Bootable Media Builder).
- Jeśli agent jest już zainstalowany, można podłączyć konsolę zarządzania do komputera, kliknąć **Pomoc > Zmień licencję** i określić klucz licencyjny lub serwer licencji, z którego należy pobrać licencję komponentu Universal Restore.

Aby nowo zainstalowany dodatek działał w środowisku startowym, należy ponownie utworzyć nośniki startowe.

5.2.2 Używanie funkcji Universal Restore

Podczas odzyskiwania

Dostępność funkcji Universal Restore podczas konfiguracji odzyskiwania dysku lub woluminu zależy od obecności systemu operacyjnego Windows lub Linux na wybranych dyskach lub woluminach. Jeśli na wybranych nośnikach znajduje się więcej niż jeden system operacyjny, funkcję Universal Restore można zastosować w odniesieniu do wszystkich systemów Windows, wszystkich systemów Linux lub systemów Windows i Linux naraz.

Jeśli program nie może wykryć, czy w kopii zapasowej jest system operacyjny, zasugeruje użycie funkcji Universal Restore na wypadek obecności systemu w kopii. Możliwe są następujące warianty takiej sytuacji:

- kopia zapasowa jest podzielona na kilka plików;
- kopia zapasowa znajduje się w skarbonie deduplikacji, w magazynie Acronis Online Backup Storage, na serwerze FTP/SFTP, taśmie, albo płycie CD lub DVD.

Czasami funkcja Universal Restore jest stosowana w tle, ponieważ program zna listę sterowników lub modułów wymaganych w przypadku obsługiwanych maszyn wirtualnych. Możliwe są następujące warianty takiej sytuacji:

- odzyskiwanie systemu na nową maszynę wirtualną;
- odzyskiwanie systemu na dowolną maszynę wirtualną za pomocą agenta Agent for ESX(i) lub Agent for Hyper-V.

Funkcja Universal Restore jest niedostępna w następujących przypadkach:

- kopia zapasowa znajduje się w strefie Acronis Secure Zone;
- korzystanie z funkcji Acronis Active Restore (s. 375);

Dzieje się tak dlatego, że te funkcje są przeznaczone głównie do natychmiastowego odzyskiwania danych na tym samym komputerze.

Bez odzyskiwania

Pod kontrolą nośnika startowego funkcję Universal Restore można zastosować również bez opcji odzyskiwania, klikając **Zastosuj funkcję Universal Restore** na ekranie powitalnym nośnika. Funkcja Universal Restore zostanie zastosowana w odniesieniu do systemu operacyjnego, który jest już zainstalowany na komputerze. Jeśli na komputerze jest kilka systemów operacyjnych, zostanie wyświetlony monit z prośbą o wybór tego, wobec którego ma zostać zastosowana funkcja Universal Restore.

Funkcja Universal Restore w systemie Windows

Przygotowanie

Przygotowanie sterowników

Przed zastosowaniem funkcji Universal Restore w systemie operacyjnym Windows upewnij się, że masz sterowniki kontrolera nowego dysku twardego i chipsetu. Sterowniki mają zasadnicze znaczenie dla uruchomienia systemu operacyjnego. Skorzystaj z płyty CD lub DVD dostarczonej przez producenta sprzętu albo pobierz sterowniki z jego witryny internetowej. Pliki sterowników powinny mieć rozszerzenia *.inf, *.sys lub *.oem. W przypadku pobrania sterowników w formacie *.exe, *.cab lub *.zip, wyodrębnij je za pomocą aplikacji innej firmy.

Najlepszą praktyką jest przechowywanie sterowników do wszystkich urządzeń używanych w przedsiębiorstwie w jednym repozytorium uporządkowanym według typu urządzenia lub według konfiguracji sprzętowych. Kopię repozytorium można przechowywać na płycie DVD lub dysku flash. Można również wybrać niektóre sterowniki i dodać je do nośnika startowego bądź utworzyć niestandardowy nośnik startowy z koniecznymi sterownikami (oraz niezbędną konfiguracją sieciową) dla każdego serwera. Można również określać ścieżkę do repozytorium podczas każdego korzystania z narzędzia Universal Restore.

Sprawdzenie dostępu do sterowników w środowisku startowym

Praca z nośnikiem startowym wymaga dostępu do urządzenia ze sterownikami. Nawet w przypadku skonfigurowania odzyskiwania dysku systemowego w środowisku systemu Windows po ponownym uruchomieniu komputera odzyskiwanie będzie przebiegać w środowisku opartym na systemie Linux. Użyj nośnika opartego na środowisku WinPE, jeśli urządzenie jest dostępne w systemie Windows, ale nośnik oparty na systemie Linux go nie wykrywa.

Postępowanie w przypadku braku sterowników

System Windows 7 zawiera więcej sterowników niż starsze wersje systemów Windows. Z dużym prawdopodobieństwem funkcja Universal Restore znajdzie wszystkie wymagane sterowniki w folderze sterowników systemu Windows 7. Być może nie będzie trzeba określać zewnętrznej ścieżki do sterowników. Niemniej dla poprawnego działania funkcji Universal Restore użycie przez system właściwych sterowników ma kluczowe znaczenie.

*Domyślny folder przechowywania sterowników w systemie Windows jest określony przez wartość **DevicePath**, którą można znaleźć w kluczu rejestru **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Zwykle jest to folder **WINDOWS\inf**.*

Ustawienia funkcji Universal Restore

Automatyczne wyszukiwanie sterowników

Określ, gdzie program powinien szukać sterowników warstwy abstrakcji sprzętowej (HAL), kontrolera dysku HDD i sterownika lub sterowników karty sieciowej:

- Jeśli sterowniki znajdują się na płycie producenta lub innym nośniku wymiennym, włącz funkcję **Przeszukaj nośniki wymienne**.
- Jeśli nośniki znajdują się w folderze sieciowym lub na nośniku startowym, określ ścieżkę do folderu, klikając **Dodaj folder**.

Podczas odzyskiwania narzędzie Universal Restore wykonuje wyszukiwanie rekursywne we wszystkich podfolderach określonego folderu, znajduje wśród dostępnych sterowników najbardziej odpowiednie sterowniki HAL i kontrolera dysku twardego, a następnie instaluje je w odzyskanym systemie. Narzędzie Universal Restore wyszukuje również sterownik karty sieciowej i przesyła

ścieżkę znalezionego sterownika do systemu operacyjnego. Jeśli sprzęt zawiera wiele kart interfejsu sieciowego, narzędzie próbuje skonfigurować sterowniki wszystkich kart.

Sterowniki pamięci masowej do zainstalowania

Ustawienie to jest dostępne po rozwinięciu sekcji **Pokaż sterowniki pamięci masowej do zainstalowania**.

Należy z niego skorzystać, jeśli:

- docelowy sprzęt zawiera określony kontroler pamięci masowej, na przykład RAID (zwłaszcza NVIDIA RAID) lub kartę Fibre Channel;
- system jest odzyskiwany na maszynę wirtualną korzystającą z kontrolera dysku twardego SCSI i uruchamianą z nośnika startowego. Użyj sterowników SCSI dołączonych do oprogramowania do wirtualizacji lub pobierz najnowsze wersje sterowników z witryny internetowej producenta oprogramowania.
- Jeśli automatyczne wyszukiwanie sterowników nie pomoże w uruchomieniu systemu.

Określ odpowiednie sterowniki, klikając **Dodaj sterownik**. Sterowniki określone w tym miejscu program zainstaluje z ewentualnymi ostrzeżeniami, nawet jeśli znajdzie lepszy sterownik.

Proces odzyskiwania

Jeśli funkcja Universal Restore nie znajdzie kompatybilnego sterownika w określonych lokalizacjach, wyświetli monit z nazwą urządzenia sprawiającego problemy. Wykonaj jedną z następujących czynności:

- Dodaj sterownik do dowolnej z wcześniej określonych lokalizacji i kliknij **Ponów**.
- Jeśli nie pamiętasz jego lokalizacji, kontynuuj odzyskiwanie. Jeśli rezultat nie będzie satysfakcjonujący, uruchom funkcję Universal Restore bez opcji odzyskiwania, klikając **Zastosuj funkcję Universal Restore** na ekranie powitalnym nośnika. Podczas konfigurowania operacji określ wymagany sterownik.

System Windows po uruchomieniu rozpoczyna standardową procedurę instalowania nowego sprzętu. Jeśli sterownik karty sieciowej ma podpis Microsoft Windows, system instaluje go w trybie dyskretnym. W przeciwnym razie system wyświetla monit o potwierdzenie instalacji niepodpisanego sterownika.

Następnie można skonfigurować połączenie sieciowe i określić sterowniki karty graficznej, złącza USB i innych urządzeń.

Funkcja Universal Restore w systemie Linux

Po uruchomieniu funkcji Universal Restore w systemie operacyjnym Linux aktualizuje ona tymczasowy system plików określany jako pierwotny dysk RAM (initrd). Dzięki temu system operacyjny można uruchomić na nowym sprzęcie.

Funkcja Universal Restore dodaje do pierwotnego dysku RAM moduły dla nowego sprzętu (w tym sterowniki urządzeń). Wymagane moduły zwykle znajduje w katalogu **/lib/modules** odzyskiwanego systemu operacyjnego. Jeśli funkcja Universal Restore nie może znaleźć któregoś z modułów, zapisuje nazwę jego pliku w dzienniku (s. 293).

Funkcja Universal Restore może zmodyfikować konfigurację programu ładującego GRUB. Tak modyfikacja może na przykład umożliwić uruchamianie systemu na nowym komputerze z innym układem woluminów niż komputer oryginalny.

Funkcja Universal Restore nigdy nie modyfikuje jądra systemu Linux.

Przywracanie oryginalnego pierwotnego dysku RAM

Program umożliwia przywrócenie w razie potrzeby oryginalnego pierwotnego dysku RAM.

Pierwotny dysk RAM jest przechowywany w postaci pliku na komputerze. Przed pierwszą aktualizacją pierwotnego dysku RAM funkcja Universal Restore zapisuje jego kopię w tym samym katalogu. Nazwa kopii stanowi połączenie nazwy pliku i przyrostka **_acronis_backup.img**. Kilkakrotne uruchomienie funkcji Universal Restore (na przykład po dodaniu brakujących sterowników) nie spowoduje zastąpienia tej kopii.

Aby przywrócić oryginalny pierwotny dysk RAM, wykonaj jedną z następujących czynności:

- Odpowiednio zmień nazwę kopii. W tym celu możesz uruchomić 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 konfiguracji programu ładującego GRUB (s. 163) zawierającym polecenie **initrd**.

Stosowanie funkcji Universal Restore w odniesieniu do wielu systemów operacyjnych

Podczas odzyskiwania funkcja Universal Restore może być stosowana w odniesieniu do następujących typów systemów operacyjnych: wszystkie systemy Windows, wszystkie systemy Linux lub jedne i drugie.

Jeśli zaznaczone do odzyskania woluminy zawierają wiele systemów Windows, można określić wszystkie wymagane dla nich sterowniki na jednej liście. Każdy sterownik zostanie zainstalowany w systemie operacyjnym, dla którego jest przeznaczony.

5.3 Odzyskiwanie systemów opartych na systemie BIOS w systemach opartych na technologii UEFI i na odwrót

Program Acronis Backup & Recovery 11 obsługuje transfer systemów operacyjnych Windows między sprzętem opartym na systemie BIOS i sprzętem obsługującym system Unified Extensible Firmware Interface (UEFI).

Ważne: Podczas migracji systemów na sprzęt oparty na technologii UEFI należy korzystać z nośników startowych opartych na systemie Linux, ponieważ nośniki startowe oparte na środowisku PE i serwer Acronis PXE Server nie obsługują technologii UEFI.

5.3.1 Odzyskiwanie woluminów

Załóżmy, że utworzono kopię zapasową systemu oraz woluminów startowych (lub całego komputera) i chcesz odzyskać te woluminy na innej platformie. Możliwość uruchamiania odzyskanego systemu zależy od następujących czynników:

- **Źródłowy system operacyjny:** system umożliwiający konwersję lub nie umożliwiający jej. Następujące systemy operacyjne Microsoft Windows umożliwiają konwersję, czyli pozwalają na zmienianie trybu uruchamiania z systemu BIOS na technologię UEFI i na odwrót:
 - Windows Vista x64 z dodatkiem SP1 i nowsze.

- Windows Server 2008 x64 z dodatkiem SP1 i nowsze.
- Windows 7 x64.
- Windows Server 2008 R2 x64.

Żadne pozostałe systemy operacyjne nie umożliwiają konwersji.

- **Styl partycji dysku źródłowego i docelowego:** MBR lub GPT. Woluminy systemowe i startowe platform BIOS korzystają z dysków MBR. Woluminy systemowe i startowe platform UEFI korzystają z dysków GPT.

W przypadku wyboru niezainicjowanego dysku docelowego do odzyskiwania zostanie on automatycznie zainicjowany jako dysk GPT lub MBR w zależności od stylu partycjonowania dysku oryginalnego, aktualnego trybu uruchamiania (UEFI lub BIOS) oraz typu systemów operacyjnych (umożliwiające konwersję lub jej nie umożliwiające) znajdujących się na tym woluminie.

Jeśli inicjowanie mogłoby spowodować utratę możliwości uruchamiania, program pobierze styl partycjonowania z woluminu źródłowego, ignorując rozmiar dysku docelowego. W takich przypadkach program może wybrać styl partycjonowania MBR dla dysków o rozmiarach przekraczających 2 TB, ale użytkownik nie będzie mógł korzystać z obszaru wykraczającego poza granicę 2 TB.

Jeśli jest to wymagane, możesz ręcznie zainicjować dysk docelowy za pomocą funkcji Zarządzanie dyskami (s. 264).

W poniższej tabeli zestawiono informacje o zachowaniu możliwości uruchamiania systemu podczas odzyskiwania woluminów startowych i systemowych systemu opartego na systemie BIOS do systemu opartego na technologii UEFI i na odwrót.

- Znak plusa (+) na zielonym tle oznacza, że system zachowa możliwości uruchamiania. Użytkownik nie musi wykonywać żadnej czynności.
- Znak plusa (+) na żółtym tle oznacza, że umożliwienie uruchamiania systemu wymaga wykonania dodatkowych czynności.
- Znak minusa (-) na czerwonym tle oznacza, że nie będzie można uruchamiać systemu z powodu ograniczeń platform BIOS i UEFI.

System oryginalny	Sprzęt docelowy			
	BIOS Dysk: MBR	BIOS Dysk: GPT	UEFI Dysk: MBR	UEFI Dysk: GPT
BIOS System operacyjny: umożliwia konwersję	+	- Rozwiązanie Odzyskaj system operacyjny na dysk MBR.	+ Dodatkowe czynności 1. Przed rozpoczęciem odzyskiwania wyłącz tryb UEFI w systemie BIOS. 2. Przeprowadź odzyskiwanie pod kontrolą nośnika startowego. lub Po zakończeniu odzyskiwania wyłącz tryb UEFI w systemie BIOS. W innych przypadkach systemu operacyjnego nie będzie można uruchomić.	+ System operacyjny umożliwiający konwersję zostanie automatycznie skonwertowany do obsługi uruchamiania w trybie UEFI.
BIOS System operacyjny: nie umożliwia konwersji				- Rozwiązanie Odzyskaj system operacyjny na dysk MBR.
UEFI System operacyjny: umożliwia konwersję	+ System operacyjny umożliwiający konwersję zostanie automatycznie skonwertowany do obsługi uruchamiania w trybie BIOS.	+ Dodatkowe czynności 1. Przed rozpoczęciem odzyskiwania włącz tryb UEFI w systemie BIOS. 2. Przeprowadź odzyskiwanie pod kontrolą nośnika startowego. lub Po zakończeniu odzyskiwania włącz tryb UEFI w systemie BIOS. W innych przypadkach systemu operacyjnego nie będzie można uruchomić.	- Rozwiązanie Odzyskaj system operacyjny na dysk GPT.	+
UEFI System operacyjny: nie umożliwia konwersji	- Rozwiązanie Odzyskaj system operacyjny na dysk GPT.			

5.3.2 Odzyskiwanie dysków

Założmy, że utworzono kopię zapasową całego dysku (ze wszystkimi jego woluminami) i chcesz go odzyskać na innej platformie docelowej.

Możliwość uruchamiania odzyskanego systemu w innych trybach zależy od rodzajów systemów operacyjnych zainstalowanych na dysku źródłowym. Systemy operacyjne mogą **umożliwiać konwersję**, tj. pozwalać na zmianę trybu uruchamiania z BIOS na UEFI i na odwrót, lub mogą **nie umożliwiać konwersji**. Aby poznać listę systemów operacyjnych umożliwiających konwersję, zobacz Odzyskiwanie woluminów (s. 149).

- Jeśli dysk źródłowy zawiera jeden lub więcej systemów operacyjnych i *wszystkie* z nich umożliwiają konwersję, tryb uruchamiania można zmienić automatycznie. W zależności od bieżącego trybu uruchamiania dysk docelowy może być zainicjowany w stylu partycjonowania GPT lub MBR.
- Jeśli *co najmniej jeden* system operacyjny na dysku źródłowym nie umożliwia konwersji (lub dysk źródłowy zawiera jakiegokolwiek woluminy startowe systemów operacyjnych nie umożliwiających konwersji), tryb uruchamiania nie można zmienić automatycznie, a program zainicjuje dysk docelowy tak jak dysk źródłowy. Aby uruchomić komputer docelowy, należy ręcznie włączyć/wyłączyć tryb UEFI w systemie BIOS. W przeciwnym razie system nie uruchomi się po odzyskaniu.

W poniższej tabeli zestawiono wszystkie przypadki odzyskiwania dysków systemu opartego na systemie BIOS na system oparty na technologii UEFI i na odwrót.

- Znak plusa (+) na zielonym tle oznacza, że dysk źródłowy zostanie odzyskany bez żadnych ograniczeń.
- Znak plusa (+) na żółtym tle oznacza, że dysk źródłowy zostanie odzyskany z pewnymi ograniczeniami. Aby pokonać te ograniczenia, może być konieczne wykonanie pewnych dodatkowych czynności.
- Znaki plusa/minusa (+/-) na czerwonym tle oznaczają, że dysk zostanie odzyskany, ale mogą wystąpić pewne problemy.

System oryginalny	Sprzęt docelowy			
	Platforma: BIOS Dysk docelowy < 2 TB	Platforma: BIOS Dysk docelowy > 2 TB	Platforma: UEFI Dysk docelowy < 2 TB	Platforma: UEFI Dysk docelowy > 2 TB
BIOS System operacyjny: umożliwia konwersję	+	+	+	+
	Dysk źródłowy zostanie odzyskany bez żadnych modyfikacji.	Dysk docelowy zostanie zainicjowany jako MBR. Ograniczenie: będzie można korzystać tylko z 2 TB miejsca na dysku. Aby pokonać ograniczenie: 1. Włącz tryb UEFI w systemie BIOS. 2. Uruchom komputer z nośnika startowego i przeprowadź odzyskiwanie. W wyniku tej operacji odzyskany system operacyjny zostanie skonwertowany tak, aby podczas uruchamiania używał technologii UEFI.	Dysk docelowy zostanie zainicjowany jako GPT. System operacyjny na odzyskanym dysku zostanie automatycznie skonwertowany do obsługi uruchamiania w trybie UEFI. Uwaga: Jeśli chcesz odzyskać dysk źródłowy w trybie „bez zmian”: 1. Wyłącz tryb UEFI w systemie BIOS*. 2. Uruchom komputer z nośnika startowego i przeprowadź odzyskiwanie.	Dysk docelowy zostanie zainicjowany jako GPT. System operacyjny na odzyskanym dysku zostanie automatycznie skonwertowany do obsługi uruchamiania w trybie UEFI.

System oryginalny	Sprzęt docelowy			
	Platforma: BIOS Dysk docelowy < 2 TB	Platforma: BIOS Dysk docelowy > 2 TB	Platforma: UEFI Dysk docelowy < 2 TB	Platforma: UEFI Dysk docelowy > 2 TB
BIOS System operacyjny: nie umożliwia konwersji	<p>+</p> <p>Dysk źródłowy zostanie odzyskany bez żadnych modyfikacji.</p>	<p>+</p> <p>Dysk docelowy zostanie zainicjowany jako dysk źródłowy (MBR).</p> <p>Ograniczenie: będzie można korzystać tylko z 2 TB miejsca na dysku.</p>	<p>+/-</p> <p>Dysk docelowy zostanie zainicjowany jako dysk źródłowy (MBR).</p> <p>Dodatkowe czynności</p> <p>Po odzyskaniu wyłącz tryb UEFI w systemie BIOS*.</p> <p>Możliwy problem</p> <p>Jeśli komputer docelowy nie obsługuje systemu BIOS, po odzyskaniu system nie uruchomi się.</p>	<p>+/-</p> <p>Dysk docelowy zostanie zainicjowany jako dysk źródłowy (MBR).</p> <p>Ograniczenie: będzie można korzystać tylko z 2 TB miejsca na dysku.</p> <p>Dodatkowe czynności</p> <p>Po odzyskaniu wyłącz tryb UEFI w systemie BIOS*.</p> <p>Możliwy problem</p> <p>Jeśli komputer docelowy nie obsługuje systemu BIOS, po odzyskaniu system nie uruchomi się.</p>

System oryginalny	Sprzęt docelowy			
	Platforma: BIOS Dysk docelowy < 2 TB	Platforma: BIOS Dysk docelowy > 2 TB	Platforma: UEFI Dysk docelowy < 2 TB	Platforma: UEFI Dysk docelowy > 2 TB
UEFI System operacyjny: umożliwia konwersję	<p>+</p> <p>Dysk docelowy zostanie zainicjowany jako MBR.</p> <p>System operacyjny na odzyskanym dysku zostanie automatycznie skonwertowany do obsługi uruchamiania w trybie BIOS.</p> <p>Uwaga: Jeśli chcesz odzyskać dysk źródłowy w trybie „bez zmian”:</p> <ol style="list-style-type: none"> 1. Włącz tryb UEFI w systemie BIOS. 2. Uruchom komputer z nośnika startowego i przeprowadź odzyskiwanie. 	<p>+</p> <p>Dysk docelowy zostanie zainicjowany jako MBR.</p> <p>System operacyjny na odzyskanym dysku zostanie automatycznie skonwertowany do obsługi uruchamiania w trybie BIOS.</p> <p>Ograniczenie: będzie można korzystać tylko z 2 TB miejsca na dysku.</p>	<p>+</p> <p>Dysk źródłowy zostanie odzyskany bez żadnych modyfikacji.</p>	<p>+</p> <p>Dysk źródłowy zostanie odzyskany bez żadnych modyfikacji.</p>

System oryginalny	Sprzęt docelowy			
	Platforma: BIOS Dysk docelowy < 2 TB	Platforma: BIOS Dysk docelowy > 2 TB	Platforma: UEFI Dysk docelowy < 2 TB	Platforma: UEFI Dysk docelowy > 2 TB
UEFI System operacyjny: nie umożliwia konwersji	+/- Dysk docelowy zostanie zainicjowany jako dysk źródłowy (GPT). Dodatkowe czynności 1. Włącz tryb UEFI w systemie BIOS. 2. Uruchom komputer z nośnika startowego i przeprowadź odzyskiwanie. Możliwy problem Jeśli komputer docelowy nie obsługuje systemu UEFI, po odzyskaniu system nie uruchomi się.	+/- Dysk docelowy zostanie zainicjowany jako dysk źródłowy (GPT). Dodatkowe czynności 1. Włącz tryb UEFI w systemie BIOS. 2. Uruchom komputer z nośnika startowego i przeprowadź odzyskiwanie. Możliwy problem Jeśli komputer docelowy nie obsługuje systemu UEFI, po odzyskaniu system nie uruchomi się.	+ Dysk źródłowy zostanie odzyskany bez żadnych modyfikacji.	+ Dysk źródłowy zostanie odzyskany bez żadnych modyfikacji.

* Większość z obecnie produkowanych płyt głównych dysponuje trybem kompatybilności z systemem BIOS. Jeśli więc system nie znajdzie programu ładującego UEFI, spróbuje uruchomić system w trybie BIOS.

5.4 Acronis Active Restore

Active Restore to zastrzeżona technologia firmy Acronis, która umożliwia przywrócenie sprawności systemu niezwłocznie po rozpoczęciu jego odzyskiwania.

Użytkownicy, którzy znają już produkt Acronis Recovery for Microsoft Exchange, mogą zauważyć, że używa on funkcji Active Restore w celu zapewnienia dostępności magazynu informacji programu Exchange niezwłocznie po uruchomieniu odzyskiwania. Chociaż funkcja ta jest oparta na identycznej technologii, odzyskiwanie magazynu informacji odbywa się w inny sposób niż odzyskiwanie systemu operacyjnego, które opisano w tej sekcji.

Obsługiwane systemy operacyjne

Funkcja Acronis Active Restore jest dostępna przy odzyskiwaniu systemu Windows począwszy od wersji Windows 2000.

Ograniczenie

Jedyną obsługiwaną lokalizacją archiwum jest dysk lokalny, a dokładniej — dowolne urządzenie dostępne z poziomu systemu BIOS komputera. Może to być strefa Acronis Secure Zone, dysk twardy USB, dysk flash lub dowolny wewnętrzny dysk twardy.

Sposób działania

Podczas konfigurowania operacji odzyskiwania należy wybrać dyski lub woluminy do odzyskania z kopii zapasowej. Program Acronis Backup & Recovery 11 skanuje wybrane dyski lub woluminy w kopii zapasowej. Jeśli zostanie znaleziony obsługiwany system operacyjny, opcja Acronis Active Restore stanie się dostępna.

Jeśli opcja nie zostanie włączona, odzyskiwanie systemu będzie wykonywane w zwykły sposób, a komputer rozpocznie działanie po zakończeniu odzyskiwania.

W przypadku włączenia tej opcji zostanie ustawiona poniższa kolejność czynności do wykonania.

Po rozpoczęciu odzyskiwania systemu następuje uruchomienie systemu operacyjnego z kopii zapasowej. Komputer odzyskuje sprawność i może udostępniać niezbędne usługi. Najwyższy priorytet odzyskiwania mają dane umożliwiające obsługę żądań przychodzących. Reszta danych jest odzyskiwana w tle.

Ponieważ żądania są obsługiwane równocześnie z procesem odzyskiwania, system może działać wolniej, nawet jeśli priorytet odzyskiwania w opcjach odzyskiwania został ustawiony na **Niski**. W ten sposób czas przestoju systemu jest ograniczany do minimum kosztem tymczasowego obniżenia wydajności.

Scenariusze użycia

1. Czas bezawaryjnej pracy systemu stanowi jedno z kryteriów wydajności.

Przykłady: usługi online dla klientów, sklepy internetowe, stanowiska do głosowania.

2. Przechowywane dane zajmują znacznie więcej miejsca niż system.

Niektóre komputery służą jako urządzenia magazynujące. W takim przypadku system operacyjny zajmuje niewiele miejsca, a pozostała część dysku jest przeznaczona na dane, na przykład filmy, utwory muzyczne lub inne pliki multimedialne. Niektóre woluminy przeznaczone na dane mogą być bardzo duże w porównaniu z systemem, przez co praktycznie cały czas odzyskiwania przypada na odzyskanie plików, które mogą być potrzebne w dużo bardziej odległej przyszłości.

Jeśli zostanie wybrana opcja Acronis Active Restore, system wznowi działanie w bardzo krótkim czasie. Użytkownicy będą mogli otwierać niezbędne pliki z magazynu, podczas gdy pozostałe pliki, niewymagane natychmiast, będą odzyskiwane w tle.

Przykłady: magazyn kolekcji filmów, magazyn kolekcji muzycznej, magazyn multimedialnych.

Sposób korzystania

1. Utwórz kopię zapasową dysku lub woluminu systemowego w lokalizacji dostępnej z poziomu systemu BIOS komputera. Może to być strefa Acronis Secure Zone, dysk twardy USB, dysk flash lub dowolny wewnętrzny dysk twardy.

Jeśli system operacyjny i jego program ładujący znajdują się na różnych woluminach, w kopii zapasowej należy zawsze uwzględnić oba woluminy. Woluminy muszą być również odzyskiwane wspólnie, gdyż w przeciwnym razie istnieje duże ryzyko, że system operacyjny nie uruchomi się.

2. Utwórz nośnik startowy.
3. Jeśli wystąpi awaria systemu, uruchom komputer przy użyciu nośnika startowego. Uruchom konsolę i połącz się z agentem startowym.

4. Skonfiguruj odzyskiwanie systemu: wybierz dysk lub wolumin systemowy, a następnie zaznacz pole wyboru **Użyj funkcji Acronis Active Restore**.

Na potrzeby rozruchu i późniejszego odzyskiwania funkcja Acronis Active Restore wybierze pierwszy system operacyjny znaleziony podczas skanowania kopii zapasowej. Aby wyniki były przewidywalne, przy użyciu funkcji Active Restore nie należy odzyskiwać więcej niż jednego systemu operacyjnego. W przypadku odzyskiwania danych na komputerze z wieloma systemami operacyjnymi należy wybierać jednocześnie tylko jeden wolumin systemowy i jeden wolumin startowy.

5. Po rozpoczęciu odzyskiwania systemu następuje uruchomienie systemu operacyjnego z kopii zapasowej. Na pasku zadań pojawia się ikona funkcji Acronis Active Restore. Komputer odzyskuje sprawność i może udostępniać niezbędne usługi. Bezpośredni użytkownik widzi drzewo dysków i ikony oraz może otwierać pliki lub uruchamiać aplikacje, nawet jeśli nie zostały one jeszcze odzyskane.

Sterowniki Acronis Active Restore przechwytyują zapytania systemowe i ustawiają najwyższy priorytet odzyskiwania plików, które są wymagane do obsługi żądań przychodzących. Podczas tego odzyskiwania „w locie” trwający proces odzyskiwania zostaje przeniesiony w tło.

Nie należy wyłączać ani ponownie uruchamiać komputera aż do zakończenia odzyskiwania. Jeśli wyłączysz komputer, wszystkie zmiany dokonane w systemie od momentu ostatniego uruchomienia zostaną utracone. System nie zostanie odzyskany (nawet częściowo). W takim przypadku jedynym możliwym rozwiązaniem będzie ponowne rozpoczęcie procesu odzyskiwania z nośnika startowego.

6. Odzyskiwanie w tle jest kontynuowane do momentu odzyskania wszystkich wybranych woluminów, utworzenia wpisu dziennika i zniknięcia ikony Acronis Active Restore z paska zadań.

5.5 Jak przekonwertować kopię zapasową dysku na maszynę wirtualną

Zamiast konwertować plik TIB na plik dysku wirtualnego, co wymaga wykonania dodatkowych operacji przygotowujących dysk wirtualny do użytku, program Acronis Backup & Recovery 11 wykonuje konwersję przez odzyskanie kopii zapasowej dysku na nową, w pełni skonfigurowaną i działającą maszynę wirtualną. Konfigurując operację odzyskiwania, można przystosować konfigurację maszyny wirtualnej do własnych potrzeb.

Komponent **Acronis Backup & Recovery 11 Agent for Windows** umożliwia odzyskanie kopii zapasowej dysku (woluminu) na nową maszynę wirtualną dowolnego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) lub Red Hat Kernel-based Virtual Machine (KVM).

Program umieści pliki nowej maszyny wirtualnej w wybranym folderze. Maszynę można uruchomić przy użyciu odpowiedniego oprogramowania do wirtualizacji lub przygotować pliki maszyny do dalszego użycia. Urządzenie wirtualne Citrix XenServer Open Virtual Appliance (OVA) można zaimportować na serwer XenServer przy użyciu narzędzia Citrix XenCenter. Pliki maszyny wirtualnej Kernel-based Virtual Machine można przenieść na komputer z systemem Linux. Następnie można uruchomić na nim maszynę wirtualną za pomocą programu Virtual Machine Manager. Stację roboczą VMware można przekonwertować na otwarty format wirtualizacji (ang. open virtualization format, OVF) przy użyciu narzędzia VMware OVF.

Komponent **Acronis Backup & Recovery 11 Agent for Hyper-V** lub **Agent for ESX(i)** umożliwia odzyskanie kopii zapasowej dysku (woluminu) na nową maszynę wirtualną na odpowiednim serwerze wirtualizacji.

Wskazówka. Maszyna wirtualna Microsoft Virtual PC nie obsługuje dysków większych niż 127 GB. Firma Acronis umożliwia tworzenie maszyn wirtualnych Virtual PC o większych dyskach, dlatego możesz podłączać dyski do maszyny wirtualnej Microsoft Hyper-V.

Aby przekonwertować kopię zapasową dysku na maszynę wirtualną:

1. Połącz konsolę z serwerem zarządzania lub komputerem, na którym jest zainstalowany agent dla systemu Windows, agent dla Hyper-V lub agent dla ESX(i).
2. Kliknij **Odzyskaj**, aby otworzyć stronę **Odzyskaj dane** (s. 130).
3. Kliknij **Wybierz dane** (s. 131). Na karcie **Widok danych** lub **Widok archiwum** wybierz dyski lub woluminy do konwertowania.
4. W polu **Odzyskaj do** wybierz **Nowa maszyna wirtualna**.
5. [Tylko jeśli konsola jest podłączona do serwera zarządzania] Kliknij **Przeglądaj**. Wybierz komputer z agentem, który przeprowadzi konwersję.
6. W polu **Typ maszyny wirtualnej** określ typ i lokalizację wynikowej maszyny wirtualnej.
7. [Opcjonalnie] W obszarze **Ustawienia maszyn wirtualnych** (s. 160) możesz zmienić ścieżkę do nowej maszyny wirtualnej, jej nazwę, tryb alokowania dysku, wielkość przydzielonej pamięci oraz inne ustawienia.

W jednym folderze nie można utworzyć maszyn tego samego typu o takiej samej nazwie. W przypadku wyświetlenia komunikatu o błędzie z powodu identycznych nazw zmień nazwę maszyny wirtualnej lub jej ścieżkę.

8. Dysk docelowy dla każdego z dysków lub woluminów źródłowych i głównych rekordów startowych zostanie wybrany automatycznie. Jeśli to konieczne, możesz zmienić dyski docelowe.

W przypadku maszyny typu Microsoft Virtual PC dysk lub wolumin zawierający program ładujący systemu operacyjnego musi być odzyskany na dysk twardy 1. W przeciwnym razie nie będzie można uruchomić systemu operacyjnego. Tego błędu nie można naprawić przez zmianę kolejności urządzeń startowych w systemie BIOS, ponieważ maszyna typu Virtual PC ignoruje te ustawienia.

9. W polu **Czas odzyskiwania** określ czas rozpoczęcia zadania odzyskiwania.
10. [Opcjonalnie] W obszarze **Parametry zadania** sprawdź **Opcje odzyskiwania** i w razie potrzeby zmień ustawienia domyślne. Wybierając **Opcje odzyskiwania > Zarządzanie zasilaniem maszyn wirtualnych**, możesz określić, czy po zakończeniu odzyskiwania chcesz automatycznie uruchomić nową maszynę wirtualną. Ta opcja jest dostępna tylko wtedy, gdy nowa maszyna wirtualna jest utworzona na serwerze wirtualizacji.
11. Kliknij **OK**. Jeśli zadanie odzyskiwania jest zaplanowane na przyszłość, określ poświadczenia, z jakimi zostanie uruchomione.

Program wyświetli widok **Plany i zadania tworzenia kopii zapasowych**, w którym można sprawdzić stan i postęp zadania odzyskiwania.

Operacje po konwersji

Wynikowy komputer zawsze ma interfejs dysku SCSI i standardowe woluminy MBR. Jeśli komputer korzysta z niestandardowego programu ładującego, może wystąpić konieczność skonfigurowania tego programu, aby wskazać nowe urządzenia, i jego ponownej aktywacji. Konfigurację programu GRUB opisano w sekcji „Jak ponownie aktywować program GRUB i zmienić jego konfigurację” (s. 163).

Wskazówka. Aby zachować woluminy logiczne (LVM) na komputerze z systemem Linux, warto rozważyć inną metodę konwersji. Utwórz nową maszynę wirtualną, uruchom ją za pomocą nośnika startowego i przeprowadź operację odzyskiwania w taki sam sposób, jak na komputerze fizycznym. Strukturę woluminów logicznych można automatycznie ponownie utworzyć (s. 41) podczas odzyskiwania.

5.5.1 Wybór typu maszyny wirtualnej/serwera wirtualizacji

Nową maszynę wirtualną można utworzyć na serwerze wirtualizacji (wymaga to zainstalowania komponentu Acronis Backup & Recovery 11 Agent for Hyper-V lub Agent for ESX(i)) albo w dowolnym dostępnym folderze lokalnym lub sieciowym.

Aby wybrać serwer wirtualizacji, na którym program ma utworzyć nową maszynę wirtualną

1. Wybierz **Umieść na wybranym serwerze wirtualizacji**.
2. Wybierz serwer wirtualizacji po lewej stronie okna. Po prawej stronie okna sprawdź szczegółowe informacje na temat serwera.
3. Kliknij **OK**, aby powrócić do strony **Odzyskiwanie danych**.

Aby wybrać typ maszyny wirtualnej

1. Wybierz **Zapisz jako pliki wybranego typu maszyny wirtualnej w określonym folderze**.
2. Wybierz typ maszyny wirtualnej po lewej stronie okna. Po prawej stronie okna sprawdź szczegółowe informacje na temat wybranego typu maszyny wirtualnej.
3. Kliknij **OK**, aby powrócić do strony **Odzyskiwanie danych**.

5.5.2 Ustawienia maszyn wirtualnych

Konfigurować można poniższe ustawienia maszyn wirtualnych.

Nazwa

Nazwa domyślna: Nowa maszyna wirtualna

Wprowadź nazwę nowej maszyny wirtualnej.

Magazyn

Ustawienie początkowe: magazyn domyślny serwera wirtualizacji, jeśli nowa maszyna jest tworzona na tym serwerze. W przeciwnym razie jest to folder dokumentów bieżącego użytkownika.

Jest to miejsce, w którym zostanie utworzona nowa maszyna wirtualna. Możliwość zmiany magazynu na serwerze wirtualizacji zależy od producenta oprogramowania do wirtualizacji i jego ustawień. VMware ESX obsługuje wiele magazynów. Serwer Microsoft Hyper-V umożliwia utworzenie nowej maszyny wirtualnej w dowolnym folderze lokalnym.

Pamięć

Ustawienie początkowe: jeśli nie jest zawarte w kopii zapasowej, jest to domyślne ustawienie serwera wirtualizacji.

Jest to ilość pamięci przydzielona nowej maszynie wirtualnej. Zakres regulacji ilości pamięci zależy od sprzętu zainstalowanego w hoście, systemu operacyjnego hosta i ustawień oprogramowania do wirtualizacji. Na przykład maksymalna dozwolona ilość pamięci na potrzeby maszyn wirtualnych może wynosić 30% pamięci całkowitej.

Dyski

Ustawienie początkowe: liczba i rozmiar dysków komputera źródłowego.

Liczba dysków jest zwykle taka sama jak w komputerze źródłowym. Może być inna, jeśli z powodu ograniczeń narzuconych przez oprogramowanie do wirtualizacji program musi dodać więcej dysków

w celu pomieszczenia woluminów komputera źródłowego. W konfiguracji maszyny można dodać dyski wirtualne, a w niektórych przypadkach usunąć proponowane dyski.

Dodając nowy dysk, obok interfejsu i pojemności można również określić jego format.

- **Format elastyczny.** Dysk zajmuje tyle miejsca w pamięci masowej, ile dane na nim przechowywane. Pozwala to zaoszczędzić miejsce w pamięci masowej. Aby włączyć format elastyczny, zaznacz pole wyboru **Alokowanie elastyczne** (w środowisku ESX) lub **Dysk powiększający się dynamicznie** (w środowisku Hyper-V).
- **Format obszerny.** Dysk zajmuje całe przydzielone miejsce w pamięci masowej. Zwiększa to wydajność maszyny wirtualnej. Aby włączyć format obszerny, anuluj zaznaczenie pola wyboru **Alokowanie elastyczne** (w środowisku ESX) lub **Dysk powiększający się dynamicznie** (w środowisku Hyper-V).

Domyślnym ustawieniem jest format obszerny, jeśli komputer fizyczny został uwzględniony w kopii zapasowej. Podczas odzyskiwania z kopii zapasowej maszyny wirtualnej program próbuje odtworzyć format dysków oryginalnego komputera. Jeśli nie jest to możliwe, stosuje się format obszerny.

Implementacja maszyn Xen jest oparta na programie Microsoft Virtual PC i ma jego ograniczenia: do 3 dysków IDE i 1 procesor. Dyski SCSI nie są obsługiwane.

Procesory

Ustawienie początkowe: jeśli nie jest zawarte w kopii zapasowej lub ustawienie z kopii zapasowej jest nieobsługiwane przez serwer wirtualizacji, jest to domyślne ustawienie serwera.

Jest to liczba procesorów nowej maszyny wirtualnej. W większości przypadków jest to wartość równa jeden. Efekt przydzielenia maszynie więcej niż jednego procesora nie jest gwarantowany. Liczba procesorów wirtualnych może być ograniczona przez konfigurację procesorów hosta, oprogramowanie do wirtualizacji lub system operacyjny-gościa. Na hostach wieloprocessorowych jest na ogół dostępnych wiele procesorów wirtualnych. Wielordzeniowy procesor hosta lub technologia hyperthreading umożliwiają czasem obsługę wielu procesorów wirtualnych na hoście z jednym procesorem.

5.6 Rozwiązywanie problemów z funkcjami startowymi dysku

Jeśli w chwili tworzenia kopii zapasowej system można było uruchomić, można oczekiwać, że będzie tak również po jego odzyskaniu. Jednak informacje zapisywane i używane przez system operacyjny do uruchomienia mogą zdezaktualizować się podczas odzyskiwania, zwłaszcza w przypadku zmiany rozmiaru partycji, ich lokalizacji lub dysków docelowych. Program Acronis Backup & Recovery 11 po odzyskaniu automatycznie aktualizuje programy ładujące systemu Windows. Również inne programy ładujące mogą być naprawione, ale w pewnych przypadkach wymagają ponownej aktywacji. Zwłaszcza w przypadku odzyskiwania woluminu systemu Linux czasem konieczne jest zastosowanie poprawek lub wprowadzenie zmian dotyczących uruchamiania, aby system Linux uruchamiał i ładował się poprawnie.

Poniżej przedstawiono podsumowanie typowych sytuacji wymagających dodatkowych czynności ze strony użytkownika.

Dlaczego odzyskany system operacyjny może się nie uruchamiać

- **System BIOS komputera jest skonfigurowany do uruchamiania z innego dysku.**

Rozwiązanie: Skonfiguruj system BIOS do uruchamiania z dysku twardego, na którym znajduje się system operacyjny.

- **System został odzyskany w innej konfiguracji sprzętowej, która jest niekompatybilna z większością kluczowych sterowników zawartych w kopii zapasowej**

Rozwiązanie: Uruchom komputer przy użyciu nośnika startowego i zastosuj program Acronis Universal Restore (s. 146) do instalacji odpowiednich sterowników i modułów.

- **System Windows został odzyskany na wolumin dynamiczny, który nie może być woluminem startowym**

Rozwiązanie: Odzyskaj system Windows na wolumin standardowy, prosty lub lustrzany.

- **Wolumin systemowy został odzyskany na dysk niezawierający głównego rekordu startowego (MBR)**

Podczas konfigurowania odzyskiwania woluminu systemowego na dysk, który nie zawiera głównego rekordu startowego, program wyświetla monit, czy wraz z woluminem systemowym ma odzyskać główny rekord startowy. Opcję nieodzyskiwania należy wybrać tylko wtedy, gdy odzyskany system nie będzie uruchamiany.

Rozwiązanie: Odzyskaj wolumin ponownie wraz z głównym rekordem startowym odpowiedniego dysku.

- **System używa programu Acronis OS Selector**

Program Acronis OS Selector, który korzysta z głównego rekordu startowego (MBR) może przestać działać, ponieważ główny rekord startowy (MBR) może ulec zmianie podczas odzyskiwania systemu. Jeśli to nastąpi, należy ponownie aktywować program Acronis OS Selector w następujący sposób.

Rozwiązanie: Uruchom komputer przy użyciu nośnika startowego programu Acronis Disk Director i wybierz z menu **Narzędzia -> Aktywuj OS Selector**.

- **System używa programu GRand Unified Bootloader (GRUB) i został odzyskany z normalnej kopii zapasowej (nie z kopii surowych danych, czyli utworzonej „sektor po sektorze”)**

Pewna część programu ładującego GRUB znajduje się w kilku pierwszych sektorach dysku lub woluminu, a pozostała część — w systemie plików na jednym z woluminów. Możliwość uruchamiania systemu można przywrócić automatycznie tylko wówczas, gdy program GRUB znajduje się w kilku pierwszych sektorach dysku oraz w systemie plików, do którego możliwy jest bezpośredni dostęp. W przeciwnym razie należy ręcznie ponownie aktywować program ładujący.

Rozwiązanie: Należy ponownie aktywować program ładujący. Konieczne może być również naprawienie pliku konfiguracyjnego.

- **System używa programu Linux Loader (LILO) i został odzyskany z normalnej kopii zapasowej (nie z kopii surowych danych, czyli utworzonej „sektor po sektorze”)**

Moduł LILO zawiera wiele odwołań do bezwzględnych numerów sektorów i dlatego nie można go automatycznie naprawić z wyjątkiem sytuacji, gdy wszystkie dane zostały odzyskane do sektorów o takich samych numerach bezwzględnych jak na dysku źródłowym.

Rozwiązanie: Należy ponownie aktywować program ładujący. Konieczne może być również naprawienie pliku konfiguracyjnego z przyczyn opisanych w poprzednim akapicie.

- **Program ładujący system wskazuje na nieprawidłowy wolumin**

Może się tak zdarzyć, gdy wolumin systemowy lub startowy nie zostanie odzyskany do oryginalnej lokalizacji.

Rozwiązanie: Modyfikacja plików boot.ini lub boot\bcd pozwala naprawić ten problem w przypadku programów ładujących w systemie Windows. Program Acronis Backup & Recovery 11 robi to automatycznie i problem nie powinien wystąpić.

W przypadku programów GRUB i LILO konieczne jest poprawienie plików konfiguracyjnych GRUB. Jeśli numer partycji głównej systemu Linux uległ zmianie, zaleca się również zmianę pliku `/etc/fstab` w sposób zapewniający prawidłowy dostęp do woluminu SWAP.

■ **System Linux został odzyskany z kopii zapasowej woluminu LVM na standardowy dysk MBR**

Takiego systemu nie można uruchomić, ponieważ jego jądro próbuje zamontować główny system plików w woluminie LVM.

Rozwiązanie: Zmień konfigurację programu ładującego i plik `/etc/fstab` tak, aby menedżer LVM nie był używany, a następnie aktywuj ponownie program ładujący.

5.6.1 Jak ponownie aktywować program GRUB i zmienić jego konfigurację

Zwykle odpowiednia procedura znajduje się w podręczniku programu ładującego. W witrynie internetowej firmy Acronis znajduje się również odpowiedni artykuł bazy wiedzy.

Poniżej przedstawiono przykład ponownej aktywacji programu GRUB w przypadku odzyskiwania dysku (woluminu) systemowego na identyczny sprzęt.

1. Uruchom system Linux lub uruchom komputer z nośnika startowego, a następnie naciśnij klawisze CTRL+ALT+F2.

2. Zamontuj odzyskiwany system:

```
mkdir /mnt/system/  
mount -t ext3 /dev/sda2 /mnt/system/ # partycja główna  
mount -t ext3 /dev/sda1 /mnt/system/boot/ # partycja startowa
```

3. Zamontuj systemy plików **proc** i **dev** w odzyskiwanym systemie:

```
mount -t proc none /mnt/system/proc/  
mount -o bind /dev/ /mnt/system/dev/
```

4. Zapisz kopię pliku menu GRUB, uruchamiając jedno z następujących poleceń:

```
cp /mnt/system/boot/grub/menu.lst /mnt/system/boot/grub/menu.lst.backup
```

lub

```
cp /mnt/system/boot/grub/grub.conf /mnt/system/boot/grub/grub.conf.backup
```

5. Zmodyfikuj plik `/mnt/system/boot/grub/menu.lst` (dystrybucje Debian, Ubuntu i SUSE Linux) lub plik `/mnt/system/boot/grub/grub.conf` (dystrybucje Fedora i Red Hat Enterprise Linux) — na przykład w następujący sposób:

```
vi /mnt/system/boot/grub/menu.lst
```

6. W pliku **menu.lst** (lub odpowiednio **grub.conf**) znajdź element menu odpowiadający odzyskiwanemu systemowi. Elementy takiego menu mają następującą postać:

```
title Red Hat Enterprise Linux Server (2,6.24,4)  
root (hd0,0)  
kernel /vmlinuz-2,6.24,4 ro root=/dev/sda2 rhgb quiet  
initrd /initrd-2,6.24,4.img
```

W wierszach rozpoczynających się od **title**, **root**, **kernel** i **initrd** określone są odpowiednio:

- Tytuł elementu menu.
- Urządzenie, na którym znajduje się jądro systemu Linux — zwykle jest to partycja startowa lub partycja główna, taka jak **root (hd0,0)** w niniejszym przykładzie.
- Ścieżka do jądra na tym urządzeniu i partycja główna. W tym przykładzie ścieżka to **/vmlinuz-2.6.24.4**, a partycja główna — **/dev/sda2**. Partycję główną można określić, podając etykietę

(na przykład **root=LABEL=/**), identyfikator (w postaci **root=UUID=jakiś_uuid**) lub nazwę urządzenia (na przykład **root=/dev/sda2**).

- Ścieżka do usługi **initrd** na tym urządzeniu.

7. Zmodyfikuj plik **/mnt/system/etc/fstab**, aby poprawić nazwy wszelkich urządzeń, które zmieniły się w wyniku odzyskiwania.

8. Uruchom powłokę GRUB przy użyciu jednego z następujących poleceń:

```
chroot /mnt/system/ /sbin/grub
```

lub

```
chroot /mnt/system/ /usr/sbin/grub
```

9. Określ dysk, na którym znajduje się program GRUB. Zwykle jest to partycja startowa lub główna:

```
root (hd0,0)
```

10. Zainstaluj program GRUB. Aby na przykład zainstalować go w głównym rekordzie rozruchowym (MBR) pierwszego dysku, uruchom następujące polecenie:

```
setup (hd0)
```

11. Zamknij powłokę GRUB:

```
quit
```

12. Odmontuj zamontowane systemy plików i ponownie uruchom komputer:

```
umount /mnt/system/dev/  
umount /mnt/system/proc/  
umount /mnt/system/boot/  
umount /mnt/system/  
reboot
```

13. Ponownie skonfiguruj program ładujący, korzystając z narzędzi i dokumentacji używanej dystrybucji systemu Linux. Na przykład w dystrybucjach Debian i Ubuntu może być konieczna edycja ujętych w komentarz wierszy w pliku **/boot/grub/menu.lst**, a następnie uruchomienie skryptu **update-grub**. W przeciwnym razie zmiany mogą nie zostać uwzględnione.

5.6.2 Moduły ładujące w systemie Windows

Windows NT/2000/XP/2003

Pewna część modułu ładującego znajduje się w sektorze startowym partycji, a pozostała część w plikach **ntldr**, **boot.ini**, **ntdetect.com**, **ntbootdd.sys**. Plik **boot.ini** jest plikiem tekstowym zawierającym konfigurację modułu ładującego. Przykład:

```
[boot loader]  
timeout=30  
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS  
[operating systems]  
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"  
/noexecute=optin /fastdetect
```

Windows Vista/2008

Pewna część modułu ładującego znajduje się w sektorze startowym partycji, a pozostała część w plikach **bootmgr**, **boot\bcd**. Po uruchomieniu systemu Windows plik **boot\bcd** jest montowany w kluczu rejestru **HKLM \BCD00000000**.

5.7 Domyślne opcje odzyskiwania

Każdy agent Acronis ma swoje własne domyślne opcje odzyskiwania. Po jego zainstalowaniu domyślne opcje mają wstępnie zdefiniowane wartości określone w dokumentacji jako **ustawienia wstępne**. Podczas tworzenia zadania odzyskiwania można użyć opcji domyślnej lub zastąpić tę opcję wartością niestandardową stosowaną tylko w odniesieniu do tego zadania.

Można również dostosować opcję domyślną, zmieniając jej wartość na inną niż wstępnie zdefiniowana. Od tej pory program będzie domyślnie używał nowej wartości we wszystkich zadaniach odzyskiwania tworzonych na danym komputerze.

Aby wyświetlić i zmienić domyślne opcje odzyskiwania, podłącz konsolę do komputera zarządzanego i z górnego menu wybierz **Opcje > Domyślne opcje tworzenia kopii zapasowej i odzyskiwania > Domyślne opcje odzyskiwania**.

Dostępne opcje odzyskiwania

Zakres dostępnych opcji odzyskiwania zależy od następujących czynników:

- Środowisko działania agenta (Windows, Linux, nośnik startowy).
- Typ odzyskiwanych danych (dysk, plik).
- System operacyjny odzyskiwany z kopii zapasowej dysku (Windows, Linux).

W poniższej tabeli zestawiono dostępność opcji odzyskiwania.

	Agent dla systemu Windows		Agent dla systemu Linux		Nośnik startowy (oparty na systemie Linux lub na środowisku PE)	
	Odzyskiwani e dysków	Odzyskiwani e plików (również z kopii zapasowej dysku)	Odzyskiwani e dysków	Odzyskiwani e plików (również z kopii zapasowej dysku)	Odzyskiwani e dysków	Odzyskiwani e plików (również z kopii zapasowej dysku)
Ustawienia dodatkowe (s. 166):						
Sprawdź poprawność archiwum przed odzyskaniem	+	+	+	+	+	+
Użyj usługi FTP w trybie aktywnym	+	+	+	+	+	+
Automatycznie ponownie uruchom komputer, gdy wymaga tego odzyskiwanie	+	+	+	+	-	-
Ponownie uruchom komputer po zakończeniu odzyskiwania	-	-	-	-	+	+
Sprawdź system plików po odzyskaniu	+	-	+	-	+	-
Zmień identyfikator SID	Odzyskiwani	-	Odzyskiwani	-	Odzyskiwani	-

	Agent dla systemu Windows		Agent dla systemu Linux		Nośnik startowy (oparty na systemie Linux lub na środowisku PE)	
	Odzyskiwanie dysków	Odzyskiwanie plików (również z kopii zapasowej dysku)	Odzyskiwanie dysków	Odzyskiwanie plików (również z kopii zapasowej dysku)	Odzyskiwanie dysków	Odzyskiwanie plików (również z kopii zapasowej dysku)
po odzyskiwaniu	e systemu Windows		e systemu Windows		e systemu Windows	
Ustaw bieżącą datę i godzinę odzyskiwanych plików	-	+	-	+	-	+
Obsługa błędów (s. 168):						
Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)	+	+	+	+	+	+
W przypadku wystąpienia błędu spróbuj ponownie	+	+	+	+	+	+
Śledzenie zdarzeń:						
Dziennik zdarzeń systemu Windows (s. 168)	+	+	-	-	-	-
SNMP (s. 169)	+	+	+	+	-	-
Zabezpieczenia na poziomie plików (s. 169):						
Odzyskaj pliki z ich ustawieniami zabezpieczeń	-	+	-	+	-	+
Punkty zamontowania (s. 170)	-	+	-	-	-	-
Powiadomienia:						
E-mail (s. 170)	+	+	+	+	-	-
WinPopup (s. 171)	+	+	+	+	-	-
Polecenia poprzedzające odzyskiwanie/następujące po nim (s. 172)	+	+	+	+	Tylko PE	Tylko PE
Priorytet odzyskiwania (s. 173)	+	+	+	+	-	-

5.7.1 Ustawienia dodatkowe

Określ dodatkowe ustawienia operacji odzyskiwania, zaznaczając lub czyszcząc poniższe pola wyboru.

Sprawdź poprawność archiwum przed odzyskaniem

Ustawienie wstępne: **Wyłączone**.

Opcja określa, czy przed odzyskaniem danych z kopii zapasowej należy sprawdzić jej poprawność. Dzięki temu można się upewnić, że kopia zapasowa nie jest uszkodzona.

Użyj usługi FTP w trybie aktywnym

Ustawienie wstępne: **Wyłączone**.

Włącz tę opcję, jeśli serwer FTP obsługuje tryb aktywny i chcesz go używać do przesyłania plików.

Automatycznie ponownie uruchom komputer, gdy wymaga tego odzyskiwanie

Ta opcja jest dostępna, gdy odzyskiwanie odbywa się na komputerze z uruchomionym systemem operacyjnym.

Ustawienie wstępne: **Wyłączone**.

Opcja określa, czy komputer ma być automatycznie uruchamiany ponownie, gdy wymaga tego proces odzyskiwania. Może się tak zdarzyć w sytuacji, gdy trzeba odzyskać wolumin zablokowany przez system operacyjny.

Ponownie uruchom komputer po zakończeniu odzyskiwania

Ta opcja jest dostępna podczas pracy z nośnikiem startowym.

Ustawienie wstępne: **Wyłączone**.

Opcja umożliwia rozruch komputera w odzyskanym systemie operacyjnym bez działania użytkownika.

Sprawdź system plików po odzyskaniu

Ta opcja jest dostępna tylko podczas odzyskiwania dysków lub woluminów.

Podczas pracy z nośnikiem startowym opcja jest niedostępna dla systemu plików NTFS.

Ustawienie wstępne: **Wyłączone**.

Opcja określa, czy po odzyskaniu dysku lub woluminu ma być sprawdzana integralność systemu plików.

Zmień identyfikator SID po odzyskiwaniu

Ta opcja nie jest dostępna, gdy odzyskiwanie jest przeprowadzane na maszynę wirtualną przez komponent Acronis Backup & Recovery 11 Agent dla ESX/ESXi lub Acronis Backup & Recovery 11 Agent dla Hyper-V.

Ustawienie wstępne: **Wyłączone**.

Program Acronis Backup & Recovery 11 umożliwia wygenerowanie unikatowego identyfikatora zabezpieczeń (SID) dla odzyskanego systemu. W przypadku odzyskiwania systemu na nim samym lub tworzenia repliki systemu, która zastąpi oryginalny system, nowy identyfikator SID nie jest potrzebny. Należy go wygenerować, gdy system oryginalny i odzyskany będą pracowały jednocześnie w tej samej grupie roboczej lub domenie.

Ustaw bieżącą datę i godzinę odzyskiwanych plików

Ta opcja jest dostępna tylko podczas odzyskiwania plików.

Ustawienie wstępne: **Włączone**.

Opcja określa, czy data i godzina plików mają być odzyskiwane z archiwum, czy też do plików ma być przypisywana bieżąca data i godzina.

5.7.2 Obsługa błędów

Te opcje są dostępne w przypadku systemów operacyjnych Windows i Linux oraz nośnika startowego.

Umożliwiają one określenie sposobu obsługi błędów, które mogą wystąpić podczas odzyskiwania.

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)

Ustawienie wstępne: **Wyłączone**.

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.

W przypadku wystąpienia błędu spróbuj ponownie

Ustawienie wstępne: **Włączone**. **Liczba prób: 30**. **Odstęp między próbami: 30 sekund**.

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 sieciowa będzie niedostępna, program będzie próbował nawiązać połączenie co 30 sekund, ale nie więcej niż 5 razy. Próby zostaną wstrzymane po wznowieniu połączenia LUB po wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

5.7.3 Śledzenie zdarzeń

Zdarzenia z dziennika dotyczące operacji odzyskiwania wykonywanych na komputerze zarządzanym można duplikować w dzienniku zdarzeń aplikacji systemu Windows lub wysyłać do określonych menedżerów SNMP.

Dziennik zdarzeń systemu Windows

Ta opcja ma zastosowanie tylko w systemie operacyjnym Windows.

Ta opcja jest niedostępna podczas wykonywania operacji na nośnikach startowych.

Opcja określa, czy agenty działające na komputerze zarządzanym muszą rejestrować zdarzenia operacji odzyskiwania w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, należy uruchomić plik **eventvwr.exe** lub wybrać polecenia **Panel sterowania > Administrative tools (Narzędzia administracyjne) > Event Viewer (Podgląd zdarzeń)**). Zdarzenia do rejestrowania można filtrować.

Ustawienie wstępne: **Użyj ustawień określonych w obszarze Opcje komputera**.

Aby wybrać, czy zdarzenia operacji odzyskiwania mają być rejestrowane w dzienniku zdarzeń aplikacji systemu Windows:

Wybierz jedno z następujących ustawień:

- **Użyj ustawień określonych w obszarze Opcje komputera** — aby używać ustawienia określonego dla komputera. Aby uzyskać więcej informacji, zobacz Opcje komputera.
- **Rejestruj zdarzenia następujących typów** — aby rejestrować zdarzenia operacji odzyskiwania w dzienniku zdarzeń aplikacji. Należy określić typy zdarzeń, które mają być rejestrowane:
 - **Wszystkie zdarzenia** — rejestrowanie wszystkich zdarzeń (informacje, ostrzeżenia i błędy);
 - **Błędy i ostrzeżenia;**
 - **Tylko błędy.**
- **Nie rejestruj** — wyłączanie rejestrowania zdarzeń operacji odzyskiwania w dzienniku zdarzeń aplikacji.

Powiadomienia SNMP

Ta opcja ma zastosowanie zarówno w systemach operacyjnych Windows, jak i Linux.

Ta opcja jest niedostępna podczas wykonywania operacji na nośnikach startowych.

Opcja określa, czy agenty działające na komputerze zarządzanym muszą wysyłać zdarzenia dziennika operacji odzyskiwania do określonych menedżerów SNMP (Simple Network Management Protocol). Można wybrać typy zdarzeń, które będą wysyłane.

Aby uzyskać szczegółowe informacje na temat programu Acronis Backup & Recovery 11, zobacz „Obsługa SNMP (s. 46)”.

Ustawienie wstępne: **Użyj ustawień określonych w obszarze Opcje komputera.**

Aby wybrać, czy zdarzenia operacji odzyskiwania mają być wysyłane do menedżerów SNMP:

Wybierz jedno z następujących ustawień:

- **Użyj ustawień określonych w obszarze Opcje komputera** — aby używać ustawienia określonego dla komputera. Aby uzyskać więcej informacji, zobacz Opcje komputera.
- **Wyślij osobne powiadomienie SNMP w przypadku każdego zdarzenia odzyskiwania** — aby wysyłać zdarzenia operacji odzyskiwania do określonych menedżerów SNMP.
 - **Typy wysyłanych zdarzeń** — wybierz typy zdarzeń, które będą wysyłane: **Wszystkie zdarzenia**, **Błędy i ostrzeżenia** lub **Tylko błędy**.
 - **Nazwa/adres IP serwera** — wpisz nazwę lub adres IP hosta z uruchomioną aplikacją do zarządzania SNMP, do której będą wysyłane komunikaty.
 - **Spółeczność** — wpisz nazwę społeczności SNMP, do której należy aplikacja do zarządzania SNMP i komputer wysyłający. Typową społecznością jest „publiczna”.

Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy ustawienia są poprawne.

- **Nie wysyłaj powiadomień SNMP** — aby wyłączyć wysyłanie zdarzeń dziennika operacji odzyskiwania do menedżerów SNMP.

5.7.4 Zabezpieczenia na poziomie plików

Ta opcja ma zastosowanie tylko w przypadku odzyskiwania z kopii zapasowej plików systemu Windows na poziomie pliku.

Ta opcja określa, czy razem z plikami mają być odzyskiwane uprawnienia NTFS do plików.

Ustawienie wstępne: **Odzyskaj pliki z ich ustawieniami zabezpieczeń.**

Jeśli uprawnienia NTFS zostały zachowane podczas tworzenia kopii zapasowej (s. 115), można wybrać, czy mają one być odzyskiwane, czy też pliki powinny dziedziczyć uprawnienia NTFS z folderu, do którego są odzyskiwane.

5.7.5 Punkty zamontowania

Ta opcja jest dostępna tylko w systemie Windows w przypadku odzyskiwania danych z kopii zapasowej na poziomie pliku.

Włącz opcję **Punkty zamontowania**, aby odzyskać pliki i foldery przechowywane na zamontowanych woluminach, których kopie zapasowe zostały wykonane z włączoną opcją **Punkty zamontowania**. Aby uzyskać szczegółowe informacje dotyczące tworzenia kopii zapasowych woluminów zamontowanych lub udostępnionych w klastrze, zobacz Punkty zamontowania (s. 117).

Ustawienie wstępne: **Wyłączone.**

Ta opcja jest dostępna tylko w przypadku, gdy folder wybrany do utworzenia kopii zapasowej 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**.

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.

5.7.6 Powiadomienia

Program Acronis Backup & Recovery 11 umożliwia powiadamianie użytkowników o zakończeniu odzyskiwania pocztą e-mail lub za pomocą usługi komunikatów.

E-mail

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Opcja umożliwia otrzymywanie pocztą e-mail powiadomień o pomyślnym zakończeniu lub niepowodzeniu zadania odzyskiwania albo konieczności wykonania działań wraz z pełnym dziennikiem zadania.

Ustawienie wstępne: **Wyłączone.**

Aby skonfigurować powiadamianie pocztą e-mail

1. Zaznacz pole wyboru **Wysyłaj powiadomienia pocztą e-mail**, aby włączyć powiadamianie.
2. W sekcji **Wysyłaj powiadomienia pocztą e-mail** zaznacz odpowiednie pola wyboru.
 - **Po pomyślnym odzyskaniu danych** — powiadomienie jest wysyłane po pomyślnym zakończeniu zadania odzyskiwania.
 - **Gdy odzyskanie danych się nie powiedzie** — powiadomienie jest wysyłane, gdy zadanie odzyskiwania nie powiedzie się.
 - **Gdy jest konieczne działanie użytkownika** — aby wysłać powiadomienie w czasie operacji, gdy wymagane jest podjęcie działania przez użytkownika.

3. W polu **Adresy e-mail** wpisz adres e-mail, na który będą wysyłane powiadomienia. Można wprowadzić kilka adresów oddzielonych średnikami.
4. W polu **Temat** wpisz temat wiadomości z powiadomieniem lub pozostaw wartość domyślną.
5. W polu **Serwer SMTP** wprowadź nazwę serwera SMTP.
6. W polu **Port** ustaw port serwera SMTP. Domyślnie jest to port **25**.
7. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika.
8. W polu **Hasło** wprowadź hasło.
9. Kliknij **Dodatkowe parametry poczty e-mail**, aby skonfigurować dodatkowe parametry poczty e-mail w następujący sposób:
 - a. **Od** — wpisz adres e-mail użytkownika, od którego zostanie wysłana wiadomość. Jeśli pozostawisz to pole puste, wiadomości będą tworzone w taki sposób, jakby pochodziły z adresu docelowego.
 - b. **Użyj szyfrowania** — umożliwia włączenie szyfrowanego połączenia z serwerem poczty. Można wybrać szyfrowanie SSL lub TLS.
 - c. Niektórzy dostawcy usług internetowych umożliwiają wysłanie poczty dopiero po uwierzytelnieniu na serwerze poczty przychodzącej. Jeśli tak jest, zaznacz pole wyboru **Zaloguj się na serwerze poczty przychodzącej**, aby umożliwić korzystanie z serwera POP i skonfigurować jego ustawienia:
 - **Serwer poczty przychodzącej (POP)** — wprowadź nazwę serwera POP.
 - **Port** — ustaw port serwera POP. Domyślnie jest to port **110**.
 - **Nazwa użytkownika** — wprowadź nazwę użytkownika.
 - **Hasło** — wprowadź hasło.
 - d. Kliknij **OK**.
10. Kliknij **Wyślij próbną wiadomość e-mail**, aby sprawdzić, czy ustawienia są poprawne.

Usługa Messenger (WinPopup)

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Opcja umożliwia otrzymywanie powiadomień WinPopup o pomyślnym zakończeniu lub niepowodzeniu zadania albo konieczności wykonania działań.

Ustawienie wstępne: **Wyłączone**.

Przed skonfigurowaniem powiadomień WinPopup należy dopilnować, aby usługa Messenger była włączona na obu komputerach: wykonującym zadanie i odbierającym wiadomości.

Usługa Messenger nie jest domyślnie uruchamiana w systemach z grupy Microsoft Windows Server 2003. Zmień tryb uruchamiania usługi na Automatyczny i uruchom usługę.

Aby skonfigurować powiadomienia WinPopup:

1. Zaznacz pole wyboru **Wysyłaj powiadomienia WinPopup**.
2. W polu **Nazwa komputera** wprowadź nazwę komputera, do którego chcesz przysyłać powiadomienia. Używanie kilku nazw nie jest obsługiwane.
3. W sekcji **Wysyłaj powiadomienia** zaznacz odpowiednie pola wyboru
 - **Po pomyślnym odzyskaniu danych** — powiadomienie jest wysyłane po pomyślnym zakończeniu zadania odzyskiwania.

- **Gdy odzyskanie danych się nie powiedzie** — powiadomienie jest wysyłane, gdy zadanie odzyskiwania nie powiedzie się.
- Pole wyboru **Gdy jest konieczne działanie użytkownika** — aby wysłać powiadomienie w czasie operacji, gdy wymagane jest podjęcie działania przez użytkownika.

4. Kliknij **Wyślij próbny komunikat WinPopup**, aby sprawdzić, czy ustawienia są poprawne.

5.7.7 Polecenia poprzedzające/następujące

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux oraz w przypadku nośników startowych opartych na środowisku PE.

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 logicznych z systemem plików, błędów fizycznych lub sektorów uszkodzonych przed rozpoczęciem odzyskiwania lub po jego zakończeniu.

Program nie obsługuje poleceń interaktywnych wymagających działania użytkownika (na przykład „pause”).

Polecenia po zakończeniu odzyskiwania nie zostaną wykonane, jeśli proces odzyskiwania uruchomi ponownie komputer.

Aby określić polecenia poprzedzające/następujące

1. Włącz wykonywanie poleceń poprzedzających/następujących, zaznaczając następujące opcje:
 - **Wykonaj przed odzyskiwaniem**
 - **Wykonaj po odzyskiwaniu**
2. Wykonaj jedną z następujących czynności:
 - Kliknij **Edytuj**, aby określić nowe polecenie lub plik wsadowy.
 - Wybierz istniejące polecenie lub plik wsadowy z listy rozwijanej.
3. Kliknij **OK**.

Polecenie poprzedzające odzyskiwanie

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu odzyskiwania

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy. Program nie obsługuje poleceń interaktywnych, to znaczy poleceń wymagających działania użytkownika (na przykład „pause”).
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Pole wyboru	Wybór			
	Wybrane	Niewybrane	Wybrane	Niewybrane
Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie				

powiedzie*				
Nie przeprowadzaj odzyskiwania przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Przeprowadź odzyskiwanie dopiero po pomyślnym wykonaniu polecenia. Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia nie powiodło się.	Przeprowadź odzyskiwanie po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N/D	Przeprowadź odzyskiwanie równoległe z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

* Polecenie uznaje się za niewykonane, jeśli jego kod wyjścia jest różny od zera.

Polecenie po zakończeniu odzyskiwania

Aby określić polecenie/plik wykonywalny, które mają zostać wykonane po zakończeniu odzyskiwania

1. W polu **Polecenie** wpisz polecenie lub wyszukaj plik wsadowy.
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
4. Zaznacz pole wyboru **Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie**, jeśli pomyślne wykonanie polecenia ma znaczenie krytyczne. Polecenie uznaje się za niewykonane, jeśli jego kod wyjścia jest różny od zera. W takim przypadku wynik wykonania zadania przyjmie wartość Zakończony niepowodzeniem.
Jeśli to pole wyboru nie jest zaznaczone, wynik wykonania polecenia nie wpływa na powodzenie lub niepowodzenie wykonania zadania. Wynik wykonania polecenia można sprawdzić, przeglądając widok **Dziennik**.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest poprawne.

Polecenia po zakończeniu odzyskiwania nie zostaną wykonane, jeśli proces odzyskiwania uruchomi ponownie komputer.

5.7.8 Priorytet odzyskiwania

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Priorytet procesu uruchomionego w systemie określa ilość zasobów procesora i zasobów systemowych przydzielonych do tego procesu. Zmniejszenie priorytetu odzyskiwania spowoduje zwolnienie większej ilości zasobów dla innych aplikacji. Zwiększenie priorytetu odzyskiwania może spowodować przyspieszenie tego procesu, ponieważ wymaga od systemu przydzielenia większej ilości zasobów do aplikacji, która przeprowadza odzyskiwanie. Jednak ostateczny efekt zależy od

całkowitego wykorzystania procesora oraz innych czynników, takich jak szybkość operacji wejścia/wyjścia na dysku i ruch w sieci.

Ustawienie wstępne: **Normalny**.

Aby określić priorytet procesu odzyskiwania

Wybierz jedno z następujących ustawień:

- **Niski** — aby zminimalizować ilość zasobów wykorzystywanych przez proces odzyskiwania, pozostawiając więcej zasobów dla innych procesów uruchomionych na komputerze;
- **Normalny** — aby uruchamiać proces odzyskiwania z normalną szybkością, przydzielając zasoby na równi z innymi procesami;
- **Wysoki** — aby zmaksymalizować szybkość procesu odzyskiwania, odbierając zasoby innym procesom.

6 Przechowywanie danych w kopiach zapasowych

6.1 Skarbce

Skarbiec to lokalizacja służąca do przechowywania archiwów kopii zapasowych. W celu ułatwienia obsługi i administracji skarbiec jest powiązany z metadanymi archiwów. Odwołania do tych metadanych przyspieszają i ułatwiają operacje na archiwach i kopiach zapasowych przechowywanych w skarbcu.

Skarbiec można założyć na dysku lokalnym lub sieciowym, nośniku wymiennym albo urządzeniu taśmowym.

Nie istnieją ustawienia służące do ograniczania rozmiaru skarbca ani liczby kopii zapasowych w skarbcu. Można ograniczyć rozmiar każdego archiwum stosując czyszczenie. Jednakże całkowity rozmiar archiwów przechowywanych w skarbcu jest ograniczony przez rozmiar urządzenia przechowującego.

Dlaczego warto tworzyć skarbcę?

Zaleca się utworzenie skarbca w każdym miejscu docelowym, w którym mają być przechowywane archiwa kopii zapasowych. Zapewni to poniższe korzyści ułatwiające pracę.

Szybki dostęp do skarbca

Nie trzeba będzie pamiętać ścieżek do folderów, w których przechowywane są archiwa. Podczas definiowania planu tworzenia kopii zapasowych albo zadania wymagającego wyboru archiwum lub miejsca docelowego w archiwum dostępna będzie lista skarbców, która zapewni szybki dostęp do skarbca bez konieczności rozwijania drzewa folderów.

Łatwe zarządzanie archiwami

Skarbiec jest dostępny w panelu **Nawigacja**. Po wybraniu skarbca można przeglądać przechowywane w nim archiwa oraz wykonywać następujące operacje zarządzania archiwami:

- Pobranie listy kopii zapasowych znajdujących się w każdym archiwum
- Odzyskiwanie danych z kopii zapasowej
- Sprawdzanie zawartości kopii zapasowej
- Sprawdzenie poprawności wszystkich archiwów w skarbcu lub poszczególnych archiwów i kopii zapasowych
- Montowanie kopii zapasowej woluminu w celu skopiowania plików z kopii zapasowej na dysk fizyczny
- Bezpieczne usuwanie archiwów oraz kopii zapasowych z archiwów

Tworzenie skarbców jest stanowczo zalecane, ale nie obowiązkowe. Można nie korzystać ze skrótów i zawsze określać ścieżkę lokalizacji.


W wyniku operacji utworzenia skarbca jego nazwa zostanie dodana w sekcji **Skarbce** panelu **Nawigacja**.



Skarbce centralne i osobiste

Skarbiec centralny to lokalizacja sieciowa przydzielona przez administratora serwera zarządzania jako miejsce przechowywania archiwów kopii zapasowych. Skarbiec centralny może być zarządzany przez węzeł magazynowania (skarbiec zarządzany) lub niezarządzany.

Skarbiec osobisty to skarbiec utworzony przy użyciu bezpośredniego połączenia konsoli z komputerem zarządzanym. Skarbce osobiste są związane z konkretnym komputerem zarządzanym.

Widok „Skarbce”

 **Skarbce** (w panelu nawigacji) — najwyższy element drzewa skarbów. Klikając go, można wyświetlić skarbcie centralne i osobiste. Do wykonywania czynności w odniesieniu do dowolnego skarbca służy pasek narzędzi znajdujący się w górnej części widoku **Skarbce**. W przypadku skarbów centralnych zobacz Czynności dotyczące skarbów centralnych (s. 178). W przypadku skarbów osobistych zobacz Czynności dotyczące skarbów osobistych (s. 186).

-  **Skarbce centralne.** Skarbce tego typu są dostępne po połączeniu konsoli z komputerem zarządzanym lub serwerem zarządzania.
-  **Skarbce osobiste.** Skarbce tego typu są dostępne po połączeniu konsoli z komputerem zarządzanym.

Klikając dowolny skarbiec w drzewie skarbów, można otworzyć szczegółowy widok tego skarbca (s. 176) i wykonywać czynności w przechowywanych w nim archiwach (s. 245) i kopiach zapasowych (s. 245).

6.1.1 Korzystanie ze skarbów

W tej sekcji krótko opisano główne elementy graficznego interfejsu użytkownika wybranego skarbca oraz przedstawiono sugestie dotyczące sposobu korzystania z nich.

Sprawdzanie informacji w skarbcu

Informacje o wybranym skarbcu znajdują się w górnym panelu jego widoku. Skumulowany wykres słupkowy umożliwia oszacowanie obciążenia skarbca. Obciążenie skarbca to stosunek wolnego do zajętego miejsca w skarbcu (wykres jest niedostępny, gdy skarbiec znajduje się w bibliotece taśm). Wolne miejsce to miejsce w urządzeniu pamięci, w którym znajduje się skarbiec. Jeśli na przykład skarbiec znajduje się na dysku twardym, wolnym miejscem skarbca jest wolne miejsce odpowiedniego woluminu. Zajęte miejsce to łączny rozmiar archiwów kopii zapasowych i ich metadanych, o ile znajdują się w skarbcu.

Dostępna jest również łączna liczba archiwów i kopii zapasowych przechowywanych w skarbcu, jak i jego pełna ścieżka.

W przypadku skarbów zarządzanych można poznać nazwę węzła magazynowania zarządzającego skarbcem oraz stany operacji szyfrowania i deduplikacji (s. 224).

Przeglądanie zawartości skarbca i zaznaczanie danych

Przeglądanie zawartości skarbca i zaznaczanie danych do odzyskania umożliwiają karty **Widok danych** lub **Widok archiwum**.

Widok danych

Karta **Widok danych** umożliwia przeglądanie i zaznaczanie danych uwzględnionych w kopiach zapasowych uporządkowanych według wersji (daty i godziny utworzenia kopii). Na karcie **Widok danych** dostępne są te same funkcje wyszukiwania i katalogowania co w wykazie danych (s. 134).

Widok archiwum

Na karcie **Widok archiwum** znajdują się dane uwzględnione w kopiach zapasowych uporządkowane według archiwów. **Widok archiwum** służy do wykonywania czynności dotyczących archiwów i kopii zapasowych przechowywanych w skarbku. Aby uzyskać więcej informacji na temat tych operacji, zobacz następujące sekcje:

- Operacje na archiwach przechowywanych w skarbku (s. 245).
- Operacje na kopiach zapasowych (s. 245).
- Sortowanie, filtrowanie i konfigurowanie elementów tabeli (s. 26).

6.1.2 Skarbce centralne

Skarbiec centralny to lokalizacja sieciowa przydzielona przez administratora serwera zarządzania jako miejsce przechowywania archiwów kopii zapasowych. Skarbiec centralny może być zarządzany przez węzeł magazynowania lub być niezarządzany. Całkowita liczba i rozmiar archiwów przechowywanych w skarbku centralnym są ograniczone jedynie wielkością dostępnej pamięci masowej.

Gdy administrator serwera zarządzania utworzy skarbiec centralny, ścieżka i nazwa tego skarbca są niezwłocznie rozsyłane do wszystkich komputerów zarejestrowanych na serwerze. W grupie **Skarbce** na komputerach pojawia się skrót do skarbca. Ze skarbca centralnego mogą korzystać dowolne plany tworzenia kopii zapasowych istniejące na komputerach, w tym plany lokalne.

Na komputerze, który nie jest zarejestrowany na serwerze zarządzania, użytkownik mający uprawnienia do tworzenia kopii zapasowych w skarbku centralnym może wykonać te czynności, określając pełną ścieżkę do skarbca. Jeśli skarbiec jest zarządzany, węzeł magazynowania zarządza zarówno archiwami użytkownika, jak i innymi archiwami przechowywanymi w skarbku.

Skarbce zarządzane

Skarbiec zarządzany to skarbiec centralny zarządzany przez węzeł magazynowania.

Węzeł magazynowania wykonuje zadania czyszczenia oraz sprawdzania poprawności w odniesieniu do każdego archiwum przechowywanego w skarbku zarządzanym, tak jak to określono w planach tworzenia kopii zapasowych (s. 382). Podczas tworzenia skarbca zarządzanego administrator może określić dodatkowe operacje, które wykona węzeł magazynowania: deduplikację i szyfrowanie. Aby uzyskać więcej informacji, zobacz „Operacje wykonywane przez węzły magazynowania” (s. 213).

Każdy skarbiec zarządzany jest samowystarczalny, co oznacza, że zawiera wszystkie metadane potrzebne do zarządzania nim przez węzeł magazynowania. Skarbiec można dołączyć do innego węzła magazynowania. Nowy węzeł magazynowania pobierze metadane ze skarbca i ponownie utworzy bazę danych konieczną do zarządzania skarbcem. Aby uzyskać więcej informacji, zobacz „Dołączanie skarbca zarządzanego” (s. 184).

Dostęp do skarbców zarządzanych

Użytkownicy muszą mieć uprawnienia administratora lub użytkownika, aby uzyskać dostęp do skarbca. Administratorzy serwera zarządzania domyślnie uzyskują uprawnienia administratora. Uprawnienia dla innych użytkowników można określić podczas tworzenia lub edycji skarbca. Aby uzyskać więcej informacji, zobacz „Uprawnienia użytkownika w węźle magazynowania” (s. 215).

Skarbce niezarządzane

Skarbiec niezarządzany to skarbiec centralny, który nie jest zarządzany przy użyciu węzła magazynowania. Aby uzyskać dostęp do skarbca niezarządzanego, należy mieć uprawnienia dostępu do lokalizacji z sieci.

Wszyscy użytkownicy mający uprawnienia odczytu/zapisu plików w skarbcu niezarządzanym mogą:

- tworzyć kopię zapasową danych w skarbcu niezarządzanym,
- odzyskiwać dane z dowolnej kopii zapasowej znajdującej się w skarbcu niezarządzanym,
- przeglądać i zarządzać wszystkimi archiwami w skarbcu niezarządzanym.





Czynności dotyczące skarbców centralnych






Aby uzyskać dostęp do czynności

1. Podłącz konsolę do serwera zarządzania.
2. W panelu **Nawigacja** kliknij **Skarbce** > **Scentralizowane**.

Wszystkie opisane tutaj operacje wykonuje się przez kliknięcie odpowiednich przycisków na pasku narzędzi skarbców. Dostęp do tych operacji można również uzyskać, wybierając element **Czynności [nazwa skarbca]** w menu głównym.

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na skarbcach centralnych.

Zadanie	Czynności
Tworzenie skarbca zarządzanego lub niezarządzanego	<ol style="list-style-type: none">1. Kliknij  Utwórz.2. W polu Typ wybierz typ skarbca: Zarządzany lub Niezarządzany <p>Procedurę tworzenia skarbców centralnych opisano szczegółowo w następujących sekcjach:</p> <ul style="list-style-type: none">▪ Tworzenie zarządzanego skarbca centralnego (s. 179)▪ Tworzenie niezarządzanego skarbca centralnego (s. 183)
Edytowanie skarbca zarządzanego lub niezarządzanego	<ol style="list-style-type: none">1. Wybierz skarbiec.2. Kliknij  Edytuj. <p>W zależności od wybranego skarbca (zarządzanego lub niezarządzanego) zostanie otwarta odpowiednia strona edycji:</p> <ul style="list-style-type: none">▪ Na stronie Edytuj skarbiec zarządzany można zmienić nazwę skarbca, konta użytkownika i informacje w polu Komentarze.▪ Na stronie Edytuj skarbiec niezarządzany można zmienić nazwę skarbca i informacje w polu Komentarze.
Odłączanie skarbca zarządzanego	<ol style="list-style-type: none">1. Wybierz skarbiec.2. Kliknij  Odłącz. <p>Odłączenie skarbca powoduje usunięcie powiązania między skarbciem i węzłem magazynowania oraz usunięcie tego skarbca z graficznego interfejsu użytkownika. Wszystkie archiwa przechowywane w skarbciu pozostaną jednak niezmienione. Wykonanie planów i zadań wymagających użycia tego skarbca zakończy się niepowodzeniem.</p> <p>Odłączony skarbiec będzie można później dołączyć do tego samego lub innego węzła magazynowania.</p> <p>Uwaga. Skarbców na urządzeniach taśmowych nie można odłączyć.</p>
Dołącz wcześniej odłączony skarbiec zarządzany	<p>Kliknij  Dołącz.</p> <p>Procedurę dołączania skarbca zarządzanego do węzła magazynowania opisano szczegółowo w sekcji Dołączanie skarbca zarządzanego (s. 184).</p> <p>Uwaga. Skarbców na urządzeniach taśmowych nie można dołączać.</p>

Zadanie	Czynności
Sprawdzanie poprawności skarbca	<ol style="list-style-type: none"> Wybierz skarbiec. Kliknij  Sprawdź poprawność. <p>Nastąpi przejście do strony Sprawdzanie poprawności (s. 231) ze wstępnie wybranym skarbcem jako źródłem. Sprawdzenie poprawności skarbca polega na sprawdzeniu wszystkich archiwów w tym skarbcu.</p>
Otwieranie folderu skarbca niezarządzanego	<ol style="list-style-type: none"> Wybierz skarbiec niezarządzany. Kliknij  Eksploruj. <p>Skarbiec będzie można przeglądać przy użyciu zwykłego menedżera plików.</p>
Usuwanie skarbca	<ol style="list-style-type: none"> Wybierz skarbiec. Kliknij  Usuń. <p>Skarbiec zostanie usunięty razem z wszystkimi przechowywanymi w nim archiwami. Wykonanie planów i zadań wymagających użycia tego skarbca zakończy się niepowodzeniem.</p>
Zmiana poświadczeń użytkownika umożliwiających dostęp do skarbca	<p>Kliknij  Zmień użytkownika.</p> <p>Poświadczenia użytkownika można zmienić tylko w przypadku skarbców znajdujących się w magazynach udostępnionych.</p>
Odświeżanie informacji o skarbcu	<p>Kliknij  Odśwież.</p> <p>Podczas przeglądania zawartości skarbca można dodawać, usuwać i modyfikować jego archiwa. Kliknij Odśwież, aby w informacjach dotyczących skarbca uwzględnić najnowsze zmiany.</p>

Tworzenie zarządzanego skarbca centralnego

Aby utworzyć zarządzany skarbiec centralny, wykonaj następujące kroki.

Skarbiec

Nazwa

Określ unikatową nazwę skarbca. Utworzenie dwóch skarbców centralnych o tej samej nazwie jest zabronione.

Komentarze

[Opcjonalnie] Wprowadź charakterystyczny opis tworzonego skarbca.

Typ

Wybierz typ **Zarządzany**.

Węzeł magazynowania

Wybierz węzeł magazynowania Acronis Backup & Recovery 11 Storage Node, który będzie zarządzać skarbcem. Może być konieczne wprowadzenie poświadczeń dostępu do węzła magazynowania.

Deduplikacja

[Opcjonalnie] Określ, czy w skarbcu ma być włączona deduplikacja archiwów. Deduplikacja zmniejsza ilość miejsca zajmowaną przez archiwa oraz ruch w sieci związany z tworzeniem kopii zapasowych. Ogranicza ona rozmiar archiwów w skarbcu, eliminując nadmiarowe dane, takie jak duplikaty plików i bloków danych.

Deduplikacja nie jest możliwa na urządzeniach taśmowych.

Aby dowiedzieć się więcej na temat sposobu działania deduplikacji, zobacz sekcję Deduplikacja (s. 224).

Szyfrowanie (s. 182)

[Opcjonalnie] Określ, czy skarbiec ma być chroniony przez szyfrowanie. Wszelkie dane zapisywane w skarbcu będą szyfrowane, a wszelkie odczytywane dane będą deszyfrowane w przezroczysty sposób przez węzeł magazynowania przy użyciu klucza szyfrowania skarbcza przechowywanego w tym węźle.

Skarbca znajdującego się w urządzeniu taśmowym nie można chronić za pomocą szyfrowania.

Ścieżka (s. 181)

Określ lokalizację, w której zostanie utworzony skarbiec. Skarbce zarządzane mogą być przechowywane w udziale sieciowym, w sieci SAN, w urządzeniu NAS, w urządzeniu taśmowym lub na lokalnym dysku twardego węzła magazynowania.

Umieść bazę danych deduplikacji razem z kopiami zapasowymi (opcja dostępna tylko wtedy, gdy funkcja **Deduplikacja** jest włączona)

Baza danych deduplikacji przechowuje wartości skrótów wszystkich elementów przechowywanych w skarbcu z wyjątkiem tych, które nie mogą być poddane deduplikacji, na przykład plików zaszyfrowanych.

Jeśli skarbiec jest tworzony na lokalnym dysku węzła magazynowania, baza danych deduplikacji będzie umieszczona w tym samym skarbcu (pole wyboru **Umieść bazę danych deduplikacji razem z kopiami zapasowymi** jest zaznaczone).

Jeśli skarbiec jest tworzony w udziale sieciowym, pole wyboru **Umieść bazę danych deduplikacji razem z kopiami zapasowymi** nie jest zaznaczone, a ścieżkę do bazy danych deduplikacji trzeba określić ręcznie.

Umieszczenie bazy danych deduplikacji razem z kopiami zapasowymi może spowodować spowolnienie działania systemu. Aby zwiększyć wydajność systemu, zaleca się utworzenie bazy danych deduplikacji i skarbcza zarządzanego na różnych dyskach.

Baza danych deduplikacji (s. 181)

Określ folder na dyskach lokalnych węzła magazynowania lub w sieci SAN w celu utworzenia bazy danych deduplikacji.

Napędy

[Opcjonalnie] Jeśli skarbiec jest tworzony w urządzeniu taśmowym, określ napędy taśmowe, które mają być używane podczas tworzenia kopii zapasowych w skarbcu. Domyślnie używane będą wszystkie dostępne napędy. Kliknij **Użyj tylko następujących napędów** i zaznacz lub usuń zaznaczenie wymaganych pól wyboru.

Puła taśm

[Opcjonalnie] Jeśli skarbiec jest tworzony w urządzeniu taśmowym, określ pulę, której taśmy będą używane przez skarbiec. Domyślnie wybrana jest pula **Acronis**.

Kompatybilność wsteczna

Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Pokaż kompatybilność wsteczną**.

[Opcjonalnie] Określ, czy skarbiec ma być kompatybilny z agentami Acronis Backup & Recovery 10. W skarbcu kompatybilnym wstecznie kopie zapasowe mogą być tworzone zarówno przez agenty w wersji Acronis Backup & Recovery 10, jak i 11.

Następujące nowe funkcje obecne w programie Acronis Backup & Recovery 11 będą niedostępne w skarbcach kompatybilnych wstecznie:

— Konta użytkowników: administratorzy i użytkownicy skarbcza.

— Scentralizowany **Wykaz danych** i **Widok danych** podczas przeglądania skarbca, jeśli konsola jest podłączona do dowolnego z agentów Acronis Backup & Recovery 10.

Kompresja

[Opcjonalnie] Określ, czy magazyn danych deduplikacji ma być kompresowany. To ustawienie jest dostępne tylko w przypadku włączenia kompatybilności wstecznej i deduplikacji.

Konta użytkownika

Administratorzy skarbca (s. 182)

Dodaj grupy lub konta użytkowników, którzy będą mieć prawa administratora tego skarbca. Administratorzy skarbca mogą przeglądać wszystkie archiwa przechowywane w skarbcu i zarządzać nimi. Administratorzy Acronis Centralized Admins i członkowie grupy Administratorzy w węźle magazynowania są traktowani jako domyślni administratorzy skarbca.

Użytkownicy skarbca (s. 183)

Dodaj grupy lub konta użytkowników, którzy będą mieć prawa użytkownika tego skarbca. Użytkownicy skarbca mogą wyświetlać tylko własne archiwa w skarbcu i zarządzać nimi. Domyślnie do użytkowników skarbca jest dodawana grupa Wszyscy węzła magazynowania.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby zatwierdzić utworzenie skarbca zarządzanego.

Ścieżka skarbca

Aby określić ścieżkę, w której zostanie utworzony skarbiec zarządzany

1. Wprowadź pełną ścieżkę do folderu w polu **Ścieżka** lub wybierz odpowiedni folder w drzewie folderów. Skarbce zarządzane można zorganizować:
 - Na lokalnych dyskach twardych węzła magazynowania.
 - W udziale sieciowym.
 - W sieci SAN (Storage Area Network).
 - W magazynie NAS (Network Attached Storage).
 - W bibliotece taśm dołączonej lokalnie do węzła magazynowania.

Aby utworzyć nowy folder skarbca w wybranej lokalizacji, kliknij  **Utwórz folder**.

2. Kliknij **OK**.


Skarbiec można utworzyć wyłącznie w pustym folderze.

Nie zaleca się tworzenia zarządzanego skarbca deduplikacji na woluminie FAT32. W takich skarbcach wszystkie zdeduplikowane elementy znajdują się w dwóch potencjalnie dużych plikach. Ponieważ maksymalny rozmiar pliku w systemach plików FAT wynosi 4 GB, po osiągnięciu tego limitu węzeł magazynowania może przestać działać.

Ścieżka bazy danych deduplikacji

Aby określić ścieżkę, w której zostanie utworzona baza danych deduplikacji

1. W grupie **Foldery lokalne** węzła magazynowania wybierz żądany folder lub wprowadź jego pełną ścieżkę w polu **Ścieżka**.

Aby utworzyć nowy folder bazy danych, kliknij  **Utwórz folder**.

Zaleca się stosowanie zaleceń zawartych w sekcji „Wybór dysku bazy danych deduplikacji” rozdziału „Sprawdzone praktyki dotyczące deduplikacji” (s. 227).

2. Kliknij **OK**.

Szyfrowanie skarbca

Jeśli skarbiec jest chroniony za pomocą szyfrowania, wszystkie dane zapisywane w skarbcu są szyfrowane, a wszystkie odczytywane dane są deszyfrowane w przezroczysty sposób przez węzeł magazynowania przy użyciu klucza szyfrowania skarbca przechowywanego w tym węźle. W przypadku kradzieży nośnika danych lub uzyskania do niego dostępu przez osobę nieuprawnioną odszyfrowanie zawartości skarbca bez dostępu do węzła magazynowania będzie niemożliwe.

To szyfrowanie nie ma nic wspólnego z szyfrowaniem archiwum określonym w planie tworzenia kopii zapasowych i wykonywanym przez agenta. Jeśli archiwum jest już zaszyfrowane, szyfrowanie po stronie węzła magazynowania zostanie zastosowane po szyfrowaniu wykonanym przez agenta.

Aby ustawić ochronę skarbca za pomocą szyfrowania

1. Zaznacz pole wyboru **Szyfruj**.
2. W polu **Wprowadź hasło** wpisz hasło.
3. W polu **Potwierdź hasło** wpisz ponownie hasło.
4. Wybierz jedną z następujących opcji:
 - **AES 128** — zawartość skarbca będzie szyfrowana przy użyciu algorytmu Advanced Encryption Standard (AES) z kluczem 128-bitowym.
 - **AES 192** — zawartość skarbca będzie szyfrowana przy użyciu algorytmu AES z kluczem 192-bitowym.
 - **AES 256** — zawartość skarbca będzie szyfrowana przy użyciu algorytmu AES z kluczem 256-bitowym.
5. Kliknij **OK**.

Algorytm kryptograficzny AES działa w trybie wiązania bloków szyfrogramu (Cipher-Block Chaining — CBC) i korzysta z losowo wygenerowanego klucza o długości zdefiniowanej przez użytkownika: 128, 192 lub 256 bitów. Im większy rozmiar klucza, tym dłużej trwa szyfrowanie archiwów przechowywanych w skarbcu, ale są one lepiej zabezpieczone.

Klucz szyfrowania jest następnie szyfrowany metodą AES-256, w której jako klucz służy skrót SHA-256 hasła. Samo hasło nie jest przechowywane w żadnym miejscu na dysku — do celów weryfikacji służy skrót hasła. Dzięki tym dwupoziomowym zabezpieczeniom archiwa są chronione przed nieautoryzowanym dostępem, ale odzyskanie utraconego hasła jest niemożliwe.

Administratorzy skarbca

Administratorzy skarbca mogą tworzyć kopie zapasowe w tym skarbcu, wyświetlać i zarządzać wszystkimi archiwami w nim przechowywanymi. Domyślnie do administratorów skarbca jest dodawana grupa Administratorzy w węźle magazynowania.

Aby dodać grupę lub konta użytkowników

1. Wprowadź w osobnych polach nazwy grup lub użytkowników według następujących schematów:
 - *NazwaWyświetlana* (na przykład: **Imię Nazwisko**)
 - *NazwaUżytkownika* (na przykład: **Uzytkownik1**)
 - *NazwaObiektu@NazwaDomeny* (na przykład: **Uzytkownik1@Domena1**)
 - *NazwaDomeny\NazwaObiektu* (na przykład: **Domena1\Uzytkownik1**)
2. Po wprowadzeniu nazw kliknij **Sprawdź nazwy**. Jeśli wprowadzona nazwa zostanie znaleziona, kliknij **OK** (do momentu znalezienia nazwy przycisk **OK** jest wyłączony).

Jeśli żadne obiekty nie zostaną znalezione, usuń nazwę i wprowadź kolejną. Jeśli zostanie znalezionych kilka obiektów odpowiadających wprowadzonej nazwie, wybierz jedną z nich i kliknij **OK** lub kliknij **Anuluj** i określ kolejną nazwę.

Na początku program próbuje znaleźć wprowadzone nazwy na liście użytkowników i grup lokalnych na komputerze z zainstalowanym węzłem magazynowania. Jeśli żadne obiekty nie zostaną znalezione, program sprawdzi użytkowników i grupy domeny.

Pojawi się monit o określenie poświadczeń do konta domeny, jeśli wprowadzisz nazwę użytkownika lub grupy, której nie można sprawdzić poprzez konto domeny. Stanie się tak na przykład, jeśli użytkownik jest zalogowany przy użyciu innego konta domeny niż nazwa domeny wprowadzona w celu sprawdzenia.

Użytkownicy skarbca

Użytkownicy skarbca mogą wyświetlać tylko własne archiwa w skarbcu i zarządzać nimi. Użytkownik skarbca będący jednocześnie członkiem grupy Administratorzy na komputerze może ponadto wyświetlać wszystkie archiwa utworzone w skarbcu zarządzanym za pomocą tego komputera i zarządzać nimi. Domyślnie do użytkowników skarbca jest dodawana grupa Wszyscy w węźle magazynowania.

Aby dodać grupę lub konta użytkowników

1. Wprowadź w osobnych polach nazwy grup lub użytkowników według następujących schematów:

- *NazwaWyświetlana* (na przykład: **Imię Nazwisko**)
- *NazwaUżytkownika* (na przykład: **Uzytkownik1**)
- *NazwaObiektu@NazwaDomeny* (na przykład: **Uzytkownik1@Domena1**)
- *NazwaDomeny\NazwaObiektu* (na przykład: **Domena1\Uzytkownik1**)

2. Po wprowadzeniu nazw kliknij **Sprawdź nazwy**. Jeśli wprowadzona nazwa zostanie znaleziona, kliknij **OK** (do momentu znalezienia nazwy przycisk **OK** jest wyłączony).

Jeśli żadne obiekty nie zostaną znalezione, usuń nazwę i wprowadź kolejną. Jeśli zostanie znalezionych kilka obiektów odpowiadających wprowadzonej nazwie, wybierz jedną z nich i kliknij **OK** lub kliknij **Anuluj** i określ kolejną nazwę.

Na początku program próbuje znaleźć wprowadzone nazwy na liście użytkowników i grup lokalnych na komputerze z zainstalowanym węzłem magazynowania. Jeśli żadne obiekty nie zostaną znalezione, program sprawdzi użytkowników i grupy domeny.

Pojawi się monit o określenie poświadczeń do konta domeny, jeśli wprowadzisz nazwę użytkownika lub grupy, której nie można sprawdzić poprzez konto domeny. Stanie się tak na przykład, jeśli użytkownik jest zalogowany przy użyciu innego konta domeny niż nazwa domeny wprowadzona w celu sprawdzenia.

Tworzenie niezarządzanego skarbca centralnego

Aby utworzyć niezarządzany skarbiec centralny, wykonaj następujące kroki.

Skarbiec

Nazwa

Określ unikatową nazwę skarbca. Utworzenie dwóch skarbców centralnych o tej samej nazwie jest zabronione.

Komentarze

Wprowadź charakterystyczny opis skarbca.

Typ

Wybierz typ **Niezarządzany**.

Ścieżka (s. 184)

Określ lokalizację, w której zostanie utworzony skarbiec.

Po wykonaniu wszystkich wymaganych kroków kliknij **OK**, aby utworzyć niezarządzany skarbiec centralny.


Ścieżka skarbca

Aby określić ścieżkę, w której zostanie utworzony skarbiec niezarządzany

1. Wprowadź pełną ścieżkę do folderu w polu Ścieżka lub wybierz odpowiedni folder w drzewie folderów. Skarbce niezarządzane można zakładać:

- Magazyn Acronis Online Backup Storage
- w udziale sieciowym,
- w sieci SAN (Storage Area Network),
- w magazynie NAS (Network Attached Storage),
- na serwerze FTP lub SFTP.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejść przy użyciu programu do przechwytywania pakietów.

Aby utworzyć nowy folder dla skarbca, kliknij  Utwórz folder.

Skarbiec można utworzyć wyłącznie w pustym folderze.

2. Kliknij OK.

Dołączanie skarbca zarządzanego

Skarbiec zarządzany przez jeden węzeł magazynowania można dołączyć do innego węzła. Może to być konieczne przy wycofywaniu urządzeń węzła magazynowania z eksploatacji, po utracie tego węzła lub w celu zrównoważenia obciążenia między węzłami. W rezultacie pierwszy węzeł przestaje zarządzać skarbcem, a drugi zaczyna.

Uwaga: Osobistych, centralnych niezarządzanych i taśmowych skarbców nie można dołączać.

Aby dołączyć skarbiec zarządzany do węzła magazynowania, wykonaj następujące kroki.

Skarbiec

Węzeł magazynowania

Wybierz węzeł magazynowania Acronis Backup & Recovery 11 Storage Node, który będzie zarządzać skarbcem.

Ścieżka

Określ ścieżkę do lokalizacji, w której są przechowywane archiwa.

Baza danych skarbca

[Opcjonalnie] Baza danych skarbca zawiera metadane kopii zapasowych i archiwów przechowywanych w skarbcu. Domyślnie baza danych skarbca znajduje się w folderze %AllUsersProfile%\Acronis\BackupAndRecovery\ASN\VaultMetadataDatabases komputera z zainstalowanym węzłem magazynowania. Zwykle odłączenie skarbca od węzła magazynowania spowoduje skopiowanie bazy danych skarbca z jej domyślnej lokalizacji do tego skarbca. Program szuka bazy danych w skarbcu w momencie jego podłączenia. Po znalezieniu bazy danych jest ona automatycznie kopiowana do lokalizacji domyślnej w węźle magazynowania, do którego podłącza się skarbiec. Jeśli nie uda się znaleźć bazy danych w

skarbcu, pojawi się monit o ręczne określenie ścieżki do niej. Jeśli w określonym folderze nie będzie można znaleźć bazy danych skarbca, nowy węzeł magazynowania pobierze metadane i ponownie utworzy bazę danych w jej domyślnej lokalizacji.

Baza danych deduplikacji

[Opcjonalnie] Program automatycznie szuka bazy danych deduplikacji. Jeśli automatycznie nie można jej znaleźć, można ręcznie określić ścieżkę do niej. Jeśli bazy danych nie można znaleźć w określonym folderze, zostanie ona w nim ponownie utworzona. Odtworzenie bazy danych deduplikacji może zająć dużo czasu.

Hasło

Należy podać hasło szyfrowania do zaszyfrowanego skarbca.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby zatwierdzić dołączenie skarbca.

Jeśli znalezienie odpowiednich baz danych nie jest możliwe, procedura dołączania może trwać dłuższą chwilę, ponieważ węzeł magazynowania musi wykonać skanowanie archiwów, zapisać metadane w bazie danych oraz zdeduplikować archiwa (jeśli pierwotnie był to skarbiec deduplikacji).

6.1.3 Skarbce osobiste

Skarbiec osobisty to skarbiec utworzony przy użyciu bezpośredniego połączenia konsoli z komputerem zarządzanym. Skarbce osobiste są związane z konkretnym komputerem zarządzanym. Są one widoczne dla wszystkich użytkowników, którzy mogą zalogować się do systemu. Prawa użytkownika do tworzenia kopii zapasowych w skarbcu osobistym są zdefiniowane w jego uprawnieniach do folderu lub urządzenia, w którym znajduje się skarbiec.

Skarbiec osobisty może być przechowywany w udziale sieciowym, na serwerze FTP, na nośniku odłączanym lub wymiennym, w magazynie Acronis Online Backup Storage, w urządzeniu taśmowym lub na lokalnym dysku twardym komputera. Strefa Acronis Secure Zone jest traktowana jako skarbiec osobisty dostępny dla wszystkich użytkowników, którzy mogą zalogować się do systemu. W przypadku tworzenia kopii zapasowych wymienionych wyżej lokalizacji skarbce osobiste są tworzone automatycznie.

Skarbce osobiste mogą być używane w lokalnych planach tworzenia kopii zapasowych i zadaniach lokalnych. Scentralizowane plany tworzenia kopii zapasowych nie korzystają ze skarbców osobistych, z wyjątkiem strefy Acronis Secure Zone.

Udostępnianie skarbca osobistego

Wiele komputerów może odnosić się do tej samej lokalizacji fizycznej, np. do tego samego udostępnionego folderu. Jednak każdy z komputerów ma swój własny skrót na drzewie **Skarbce**. Użytkownicy tworzący kopie zapasowe w folderze udostępnionym mogą wyświetlać archiwa innych użytkowników i zarządzać nimi zgodnie z posiadanymi uprawnieniami dostępu do danego folderu. W celu ułatwienia identyfikacji archiwów w widoku **Skarbiec osobisty** znajduje się kolumna **Właściciel** z informacjami o właścicielach poszczególnych archiwów. Aby dowiedzieć się więcej na temat pojęcia właściciela, zobacz Właściciele i poświadczenia (s. 32).

Metadane

Folder **.meta** jest tworzony w każdym skarbcu osobistym podczas tworzenia kopii zapasowej. Jest to folder zawierający dodatkowe informacje na temat archiwów i kopii zapasowych przechowywanych w skarbcu, w tym informacje o właścicielach archiwów i nazwach komputerów. W razie przypadkowego usunięcia folderu **.meta** zostanie on utworzony ponownie w sposób automatyczny.

przy kolejnym dostępie do skarbca. Jednak niektóre informacje, takie jak nazwy właścicieli i nazwy komputerów, mogą zostać utracone.









Czynności dotyczące skarbców osobistych

Aby uzyskać dostęp do czynności

1. Podłącz konsolę do serwera zarządzania.
2. W panelu **Nawigacja** kliknij **Skarbce** > **Osobiste**.

Wszystkie opisane tutaj operacje wykonuje się przez kliknięcie odpowiednich przycisków na pasku narzędzi skarbców. Dostęp do tych operacji można również uzyskać, wybierając element **Czynności [nazwa skarbca]** w menu głównym.

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na skarbcach osobistych.

Zadanie	Czynności
Tworzenie skarbca osobistego	Kliknij  Utwórz . Procedura tworzenia skarbców osobistych jest szczegółowo opisana w sekcji Tworzenie skarbca osobistego (s. 187).
Edycja skarbca	1. Wybierz skarbiec. 2. Kliknij  Edytuj . Na stronie Edytuj skarbiec osobisty można zmienić nazwę skarbca i informacje w polu Komentarze .
Zmiana konta użytkownika umożliwiającego dostęp do skarbca	Kliknij  Zmień użytkownika . W wyświetlonym oknie dialogowym podaj poświadczenia wymagane do uzyskania dostępu do skarbca.
Tworzenie strefy Acronis Secure Zone	Kliknij  Utwórz strefę Acronis Secure Zone . Procedura tworzenia strefy Acronis Secure Zone jest szczegółowo opisana w sekcji Tworzenie strefy Acronis Secure Zone (s. 188).
Eksplorowanie zawartości skarbca	Kliknij  Eksploruj . W wyświetlonym oknie Eksploratora przejrzyj zawartość wybranego skarbca.
Sprawdzanie poprawności skarbca	Kliknij  Sprawdź poprawność . Nastąpi przejście do strony Sprawdzanie poprawności (s. 231), na której ten skarbiec będzie wstępnie wybrany jako źródło. Sprawdzenie poprawności skarbca polega na sprawdzeniu wszystkich archiwów przechowywanych w tym skarbcu.
Usuwanie skarbca	Kliknij  Usuń . Operacja usunięcia w rzeczywistości powoduje tylko usunięcie skrótu do danego folderu z widoku Skarbce . Sam folder pozostaje niezmieniony. Archiwa znajdujące się w folderze można zachować lub usunąć.
Odświeżanie informacji w tabeli skarbców	Kliknij  Odśwież . Podczas przeglądania zawartości skarbca można dodawać, usuwać i modyfikować jego archiwa. Kliknij Odśwież , aby w informacjach dotyczących skarbca uwzględnić najnowsze zmiany.

Tworzenie skarbca osobistego

Aby utworzyć skarbiec osobisty

1. W polu **Nazwa** wpisz nazwę tworzonego skarbca.
2. [Opcjonalnie] W polu **Komentarze** dodaj opis skarbca.
3. Kliknij **Ścieżka** i określ ścieżkę do folderu, który będzie służył jako skarbiec. Skarbiec osobisty może być przechowywany w udziale sieciowym, na serwerze FTP, na nośniku wymiennym, w magazynie Acronis Online Backup Storage, w urządzeniu taśmowym lub na lokalnym dysku twardym komputera.
4. [Opcjonalnie] Jeśli skarbiec jest tworzony w urządzeniu taśmowym:
 - a. Kliknij **Napędy** w celu określenia napędów taśmowych, które mają służyć do tworzenia kopii zapasowych w skarbcu. Domyślnie używane będą wszystkie dostępne napędy. Kliknij **Użyj tylko następujących napędów** i zaznacz lub usuń zaznaczenie wymaganych pól wyboru.
 - b. Kliknij **Pula taśm** i określ pulę, której taśmy będą wykorzystywane przez skarbiec. Domyślnie wybrana jest pula **Acronis**.
5. Kliknij **OK**. Utworzony skarbiec pojawi się w grupie **Osobiste** w drzewie skarbców.

Scalanie i przenoszenie skarbców osobistych

Co zrobić, aby przenieść istniejący skarbiec z jednego miejsca w inne?

Wykonaj następujące czynności

1. Upewnij się, że podczas przenoszenia plików żaden z planów tworzenia kopii zapasowych nie korzysta z istniejącego skarbca, lub wyłącz odpowiednie plany. Zobacz Czynności dotyczące planów i zadań tworzenia kopii zapasowych (s. 282).
2. Ręcznie przenieś folder skarbca z całą jego zawartością do nowego miejsca przy użyciu menedżera plików innej firmy.
3. Utwórz nowy skarbiec.
4. Edytuj plany i zadania tworzenia kopii zapasowych: przekieruj ich miejsce docelowe do nowego skarbca.
5. Usuń stary skarbiec.

W jaki sposób można scalić dwa skarbce?

Przypuśćmy, że istnieją dwa skarbce: *A* i *B*. Oba są używane w planach tworzenia kopii zapasowych. Decydujesz się pozostawić tylko skarbiec *B* i przenieść do niego wszystkie archiwa ze skarbca *A*.

W tym celu wykonaj następujące czynności

1. Upewnij się, że podczas scalania ze skarbca *A* nie korzysta żaden z planów tworzenia kopii zapasowych, lub wyłącz odpowiednie plany. Zobacz Czynności dotyczące planów i zadań tworzenia kopii zapasowych (s. 282).
2. Ręcznie przenieś zawartość foldera *A* do skarbca *B* przy użyciu osobnego menedżera plików.
3. Zmodyfikuj plany tworzenia kopii zapasowych korzystające ze skarbca *A*: jako ich miejsce docelowe wskaż skarbiec *B*.
4. W drzewie skarbców zaznacz skarbiec *B*, aby sprawdzić, czy zostaną wyświetlone archiwa. Jeśli tak się nie stanie, kliknij **Odśwież**.
5. Usuń skarbiec *A*.

6.2 Strefa Acronis Secure Zone

Strefa Acronis Secure Zone to bezpieczna partycja, która umożliwia przechowywanie archiwów kopii zapasowych na dysku zarządzanego komputera. Dzięki temu dysk można odzyskać na tym samym dysku, na którym znajduje się jego kopia zapasowa.

W przypadku fizycznej awarii dysku strefa i znajdujące się w niej archiwa zostaną utracone. Z tego powodu strefa Acronis Secure Zone nie powinna być jedyną lokalizacją do przechowywania kopii zapasowych. W infrastrukturze przedsiębiorstwa strefa Acronis 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.

Zalety

Strefa Acronis Secure Zone:

- 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 użytkownika.
- Jako wewnętrzna lokalizacja archiwum, eliminuje potrzebę użycia dodatkowego nośnika lub połączenia sieciowego w celu utworzenia kopii zapasowej lub odzyskania danych. Szczególnie przydaje się to użytkownikom urządzeń przenośnych.
- Może służyć jako lokalizacja podstawowa podczas korzystania z replikacji kopii zapasowych (s. 93).

Ograniczenia

- Strefy Acronis Secure Zone nie można zorganizować na dysku dynamicznym.

6.2.1 Tworzenie strefy Acronis Secure Zone

Strefę Acronis Secure Zone można utworzyć w działającym systemie operacyjnym lub przy użyciu nośnika startowego.

Aby utworzyć strefę Acronis Secure Zone, wykonaj poniższe czynności.

Lokalizacja i rozmiar

Dysk (s. 189)

Wybierz dysk twardy (jeśli jest ich kilka), na którym chcesz utworzyć strefę. Program tworzy strefę Acronis Secure Zone, wykorzystując nieprzydzielone miejsce na dysku lub wolne miejsce na woluminie.

Rozmiar (s. 189)

Określ dokładny rozmiar strefy. Przeniesienie lub zmiana rozmiaru zablokowanych woluminów, na przykład woluminu zawierającego aktywny system operacyjny, wymaga ponownego uruchomienia komputera.

Zabezpieczenia

Hasło (s. 189)

[Opcjonalnie] Zabezpiecz strefę Acronis Secure Zone przed nieupoważnionym dostępem przy użyciu hasła. Podczas każdej operacji związanej ze strefą pojawi się monit o podanie hasła.

Po skonfigurowaniu wymaganych ustawień kliknij OK. W oknie Potwierdzenie wyniku (s. 190) sprawdź oczekiwany układ i kliknij OK, aby rozpocząć tworzenie strefy.

Dysk strefy Acronis Secure Zone

Strefa Acronis Secure Zone może znajdować się na dowolnym stałym dysku twardym. Strefa Acronis Secure Zone jest zawsze tworzona na końcu dysku twardego. Na komputerze może istnieć tylko jedna strefa Acronis Secure Zone. Jest ona tworzona przy użyciu ewentualnego nieprzydzielonego miejsca lub wolnego miejsca na woluminie.

Strefy Acronis Secure Zone nie można zorganizować na dysku dynamicznym.

Aby przydzielić miejsce dla strefy Acronis Secure Zone

1. Wybierz dysk twardy (jeśli jest ich kilka), na którym chcesz utworzyć strefę. Domyślnie wybrane jest nieprzydzielone miejsce i wolne miejsce na wszystkich woluminach pierwszego wymienionego dysku. Program wyświetli łączną ilość miejsca dostępnego dla strefy Acronis Secure Zone.
2. Chcąc przydzielić strefie więcej miejsca, wybierz woluminy, z których ma pochodzić wolne miejsce. W zależności od dokonanego wyboru program ponownie wyświetli łączną ilość miejsca dostępnego dla strefy Acronis Secure Zone. W oknie **Rozmiar strefy Acronis Secure Zone** (s. 189) możesz ustawić dokładny rozmiar strefy.
3. Kliknij **OK**.

Rozmiar strefy Acronis Secure Zone

Wprowadź rozmiar strefy Acronis Secure Zone lub przeciągnij suwak w celu wybrania dowolnego rozmiaru między wartościami minimalną i maksymalną. Rozmiar minimalny wynosi 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, które zostały wybrane w poprzednim kroku.

Przydzielając miejsce z woluminu startowego lub systemowego, należy pamiętać o następujących kwestiach:

- Przeniesienie lub zmiana nazwy woluminu, z którego aktualnie uruchamiany jest system, wymaga ponownego uruchomienia systemu.
- Przydzielenie całego wolnego miejsca z woluminu systemowego może spowodować, że system operacyjny będzie działał niestabilnie lub nawet przestanie się uruchamiać. W przypadku wybrania woluminu startowego lub systemowego nie należy ustawiać maksymalnego rozmiaru strefy.

Hasło strefy Acronis Secure Zone

Ustawienie hasła chroni strefę Acronis Secure Zone przed nieupoważnionym dostępem. Podczas każdej operacji związanej ze strefą i znajdującymi się w niej archiwami, takiej jak tworzenie kopii zapasowej i odzyskiwanie danych, sprawdzanie poprawności archiwów, zmiana rozmiaru lub usuwanie strefy, program wyświetli monit o podanie hasła

Aby ustawić hasło

1. Wybierz **Użyj hasła**.
2. W polu **Wprowadź hasło** wpisz nowe hasło.
3. W polu **Potwierdź hasło** wpisz ponownie hasło.
4. Kliknij **OK**.

Aby wyłączyć hasło

1. Wybierz **Nie używaj**.
2. Kliknij **OK**.

Potwierdzenie wyniku

W oknie **Potwierdzenie wyniku** jest wyświetlany spodziewany układ partycji na podstawie wybranych ustawień. Jeśli układ jest zadowalający, kliknij **OK**, co spowoduje rozpoczęcie tworzenia strefy Acronis Secure Zone.

Wpływ wprowadzonych ustawień

W tej sekcji objaśniono, w jaki sposób utworzenie strefy Acronis Secure Zone wpływa na dysk zawierający wiele woluminów.

- Strefa Acronis Secure Zone jest zawsze tworzona na końcu dysku twardego. Podczas obliczania ostatecznego układu woluminów program najpierw wykorzystuje nieprzydzielone miejsce na końcu dysku.
- 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, program zajmuje wolne miejsce na woluminach wybranych przez użytkownika, zmniejszając odpowiednio rozmiary tych woluminów. Zmiana rozmiaru zablokowanych woluminów wymaga ponownego uruchomienia systemu.
- Na woluminie powinno jednak pozostać wolne miejsce, wymagane do prawidłowego działania systemu operacyjnego i aplikacji (na przykład do tworzenia plików tymczasowych). Program nie zmniejszy rozmiaru woluminu, na którym ilość wolnego miejsca jest lub stałaby się mniejsza niż 25% rozmiaru woluminu. Dopiero wówczas, gdy wszystkie woluminy na dysku będą zawierać 25% lub mniej wolnego miejsca, proporcjonalne zmniejszanie rozmiaru woluminów będzie kontynuowane.

Jak widać powyżej, nie warto ustawiać maksymalnego możliwego rozmiaru strefy. W efekcie na żadnym woluminie nie pozostanie wolne miejsce, skutkiem czego system operacyjny lub aplikacje mogą działać niestabilnie lub w ogóle się nie uruchamiać.

6.2.2 Zarządzanie strefą Acronis Secure Zone

Strefa Acronis Secure Zone jest obsługiwana jako skarbonka osobista (s. 385). Po utworzeniu na komputerze zarządzanym strefa jest zawsze obecna na liście **Skarbonki osobiste**. Strefa Acronis Secure Zone może być używana w scentralizowanych planach tworzenia kopii zapasowych, a także w planach lokalnych.

Wszystkie operacje zarządzania archiwami dostępne w skarbonkach dotyczą także strefy Acronis Secure Zone. Aby uzyskać więcej informacji na temat operacji zarządzania archiwami, zobacz Operacje na archiwach i kopiach zapasowych (s. 244).

Zwiększanie strefy Acronis Secure Zone

Aby zwiększyć strefę Acronis Secure Zone

1. Na stronie **Zarządzaj strefą Acronis Secure Zone** kliknij **Zwiększ**.
2. Wybierz woluminy, których wolne miejsce chcesz wykorzystać do zwiększenia strefy Acronis Secure Zone.

3. Określ nowy rozmiar strefy:

- Przeciągając suwak i wybierając dowolny rozmiar między wartościami bieżącą a maksymalną. Maksymalny rozmiar jest równy ilości nieprzydzielonego miejsca na dysku i łącznej ilości wolnego miejsca na wszystkich wybranych partycjach.
- Wpisując dokładną wartość w polu Rozmiar strefy Acronis Secure Zone.

Podczas zwiększania rozmiaru strefy program postępuje w poniższy sposób:

- Najpierw wykorzystuje nieprzydzielone miejsce. W razie potrzeby program przenosi woluminy, ale nie zmienia ich rozmiaru. Przeniesienie zablokowanych woluminów wymaga ponownego uruchomienia komputera.
- Jeśli ilość nieprzydzielonego miejsca jest niewystarczająca, program wykorzystuje wolne miejsce na wybranych woluminach, proporcjonalnie zmniejszając ich rozmiary. Zmiana rozmiaru zablokowanych partycji wymaga ponownego uruchomienia komputera.

Zmniejszenie rozmiaru woluminu systemowego do minimalnej wielkości może uniemożliwić uruchomienie systemu operacyjnego komputera.

4. Kliknij **OK**.

Zmniejszanie strefy Acronis Secure Zone

Aby zmniejszyć strefę Acronis Secure Zone

1. Na stronie **Zarządzaj strefą Acronis Secure Zone** kliknij **Zmniejsz**.
2. Wybierz woluminy, do których chcesz dodać wolne miejsce po zmniejszeniu strefy.
3. Określ nowy rozmiar strefy:
 - Przeciągając suwak i wybierając dowolny rozmiar między wartościami bieżącą a minimalną. Minimalny rozmiar to około 50 MB, w zależności od geometrii dysku twardego.
 - Wpisując dokładną wartość w polu **Rozmiar strefy Acronis Secure Zone**.
4. Kliknij **OK**.

Usuwanie strefy Acronis Secure Zone

Aby usunąć strefę Acronis Secure Zone:

1. Na stronie **Zarządzaj strefą Acronis Secure Zone** kliknij **Usuń**.
2. W oknie **Usuń strefę Acronis Secure Zone** wybierz woluminy, do których chcesz dodać miejsce zwolnione ze strefy, a następnie kliknij **OK**.

W przypadku wybrania kilku woluminów miejsce zostanie rozłożone proporcjonalnie na każdej partycji. W przypadku niewybrania woluminu zwolnione miejsce stanie się nieprzydzielone.

Po kliknięciu **OK** program Acronis Backup & Recovery 11 rozpocznie usuwanie strefy.

6.3 Urządzenia taśmowe

W kolejnych sekcjach szczegółowo opisano korzystanie z urządzeń taśmowych do przechowywania archiwów kopii zapasowych.

Pracę z urządzeniami taśmowymi umożliwia zaawansowana wersja programu Acronis Backup & Recovery 11 lub uaktualnienie programu Acronis Backup & Recovery 10 do programu Acronis Backup & Recovery 11.

6.3.1 Co to jest urządzenie taśmowe?

Urządzenie taśmowe to termin ogólny oznaczający bibliotekę taśm lub autonomiczny napęd taśmowy.

Biblioteka taśm (biblioteka automatyczna) to urządzenie pamięci masowej o dużej pojemności, które składa się z:

- jednego lub kilku napędów taśmowych;
- wielu (nawet kilku tysięcy) gniazd do przechowywania taśm;
- jednego lub kilku zmieniaaczy (automatów), których zadaniem jest przenoszenie taśm między gniazdami a napędami taśmowymi.

Może ona również obejmować inne komponenty, takie jak czytniki i drukarki kodów kreskowych.

Zmieniacz to szczególna odmiana bibliotek taśm. Składa się z jednego napędu, kilku gniazd, zmieniaacza i czytnika kodów kreskowych (opcjonalnie).

Autonomiczny napęd taśmowy (inaczej **streamer**) zawiera jedno gniazdo i umożliwia jednoczesne wsunięcie tylko jednej taśmy.

6.3.2 Omówienie obsługi urządzeń taśmowych

Agenty programu Acronis Backup & Recovery 11 mogą tworzyć kopie zapasowe danych na urządzeniu taśmowym bezpośrednio lub za pośrednictwem węzła magazynowania Acronis Backup & Recovery 11 Storage Node (s. 15). W obu przypadkach zapewniona jest w pełni automatyczna obsługa urządzenia taśmowego. Jeśli do węzła magazynowania podłączone jest urządzenie taśmowe z kilkoma napędami, możliwe jest jednoczesne tworzenie kopii zapasowych na taśmach za pomocą wielu komputerów.

Kompatybilność z oprogramowaniem RSM i programami innych firm

Współistnienie z oprogramowaniem innych firm

Program Acronis Backup & Recovery 11 nie może korzystać z taśm na komputerze z zainstalowanym programem innej firmy, zawierającym zastrzeżone narzędzia do zarządzania taśmami. Korzystanie przez program Acronis Backup & Recovery 11 z taśm na takim komputerze wymaga odinstalowania lub dezaktywacji programu innej firmy do zarządzania taśmami.

Współpraca z menedżerem RSM

W odróżnieniu od programu Acronis Backup & Recovery 10 do pracy programu Acronis Backup & Recovery 11 nie jest wymagany Menedżer magazynu wymiennego systemu Windows. W trakcie uaktualniania z wersji Acronis Backup & Recovery 10 program Acronis Backup & Recovery 11 zapisuje niezbędne informacje z menedżera RSM we własnej bazie danych w nowym formacie.

Po wykryciu urządzenia taśmowego (s. 200) program Acronis Backup & Recovery 11 uniemożliwia jego wykorzystanie przez menedżera RSM (chyba że urządzenia taśmowego używa inny program). Upewnij się, że przez cały czas planowanego korzystania z urządzenia taśmowego przez program Acronis Backup & Recovery 11 nie zostanie ono włączone w menedżerze RSM przez użytkownika lub program innej firmy. Jeśli urządzenie zostanie włączone w menedżerze RSM, powtórz wykrywanie urządzenia taśmowego.

Obsługiwany sprzęt

Program Acronis Backup & Recovery 11 obsługuje zewnętrzne urządzenia SCSI. Są to urządzenia podłączane do sieci Fibre Channel lub używające interfejsów SCSI, iSCSI, Serial Attached SCSI (SAS). Nie gwarantuje się możliwości rozpoznawania urządzeń podłączonych do interfejsu USB, IDE lub SATA. Zależy ona od instalacji odpowiednich sterowników w systemie operacyjnym.

Baza danych zarządzania taśmami

Program Acronis Backup & Recovery 11 przechowuje informacje o wszystkich urządzeniach taśmowych dołączonych do komputera w bazie danych zarządzania taśmami. Domyślna ścieżka bazy danych to %AllUsersProfile%\Application Data\Acronis\BackupAndRecovery\ARSM\Database.

Rozmiar bazy danych zależy od liczby archiwów przechowywanych na taśmach i wynosi około 10 MB na sto archiwów. Baza danych może osiągnąć bardzo duży rozmiar, jeśli biblioteka taśm zawiera tysiące archiwów. W takim przypadku dobrym rozwiązaniem może być zapisanie bazy danych taśm na innym woluminie.

W celu przeniesienia bazy danych:

1. Zatrzymaj usługę Acronis Removable Storage Management.
2. Przenieś wszystkie pliki z lokalizacji domyślnej do nowej.
3. Dodaj klucz rejestru opisany poniżej. Określ ścieżkę nowej lokalizacji w wartości rejestru **TapesDatabasePath**.

Klucz rejestru: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings

Wartość rejestru: **TapesDatabasePath**

Możliwe wartości danych: Dowolny ciąg znaków o długości od 0 do 32765 znaków.

Opis: Określa folder, gdzie znajduje się baza danych zarządzania taśmami.

4. Uruchom usługę Acronis Removable Storage Management.

Właściwości tworzenia kopii zapasowych na taśmach

Opcje tworzenia kopii zapasowych

Można skonfigurować opcje tworzenia kopii zapasowych **Zarządzanie taśmami** (s. 124) określające:

- kiedy wysunąć taśmę;
- czy używać wolnej taśmy do każdej pełnej, przyrostowej lub różnicowej kopii zapasowej;
- czy zastępować taśmę w napędzie podczas tworzenia pełnej kopii zapasowej (dotyczy tylko autonomicznych napędów taśmowych);
- czy używać osobnego zestawu taśm do tworzenia kopii zapasowej każdego komputera.

Schematy tworzenia kopii zapasowych

Schemat prosty

W przypadku korzystania z prostego schematu tworzenia kopii zapasowych (s. 55) na taśmach można tworzyć tylko pełne kopie zapasowe. Jest to związane z niedostępnością opcji konsolidacji (s. 380) kopii zapasowych przechowywanych na taśmach. W przypadku istnienia opcji tworzenia przyrostowych kopii zapasowych nie można byłoby usunąć żadnej z zapisanych kopii.

Schematy Dziadek-ojciec-syn oraz Wieża Hanoi

Domyślnie schematy Dziadek-ojciec-syn (s. 56) oraz Wieża Hanoi (s. 62) umożliwiają tworzenie na taśmach jedynie pełnych kopii zapasowych. Ułatwia to punktualne usuwanie przez program każdej z kopii zapasowych zgodnie z definicją zawartą w schemacie tworzenia kopii zapasowych.

Domyślne ustawienie można zmienić, aby umożliwić tworzenie pełnych, przyrostowych i różnicowych kopii zapasowych. Na przykład w przypadku posiadania kilku taśm i dużego rozmiaru pełnych kopii zapasowych może wystąpić konieczność zaoszczędzenia miejsca na taśmach.

Każdy poziom powyższych schematów korzysta z osobnego zestawu taśm w ramach tej samej puli taśm. Oznacza to, że program może jedynie korzystać z taśmy należącej do określonego zestawu taśm lub z wolnej taśmy (jeśli na aktualnie używanej taśmie kończy się miejsce). Ułatwia to zmniejszenie liczby używanych taśm, ponieważ taśmy z przyrostowymi i różnicowymi kopiami zapasowymi są częściej zapełniane i ponownie zapisywane niż te zawierające pełne kopie zapasowe.

Schemat niestandardowy

Skonfiguruj schemat niestandardowy, który będzie tworzył pełne kopie zapasowe z rozsądną częstotliwością. W przeciwnym razie, jeśli określisz reguły przechowywania, program nie będzie mógł odpowiednio zastępować zawartości taśm.

W regułach przechowywania Niestandardowego schematu tworzenia kopii zapasowych (s. 59) opcja **Jeśli kopia zapasowa do przeniesienia lub usunięcia ma zależności: Konsoliduj te kopie zapasowe** jest wyłączona. Dostępna jest jedynie opcja **Przechowuj kopię zapasową, dopóki nie zostaną usunięte wszystkie zależne kopie zapasowe**. Jest to związane z niedostępnością opcji konsolidacji (s. 380) kopii zapasowych przechowywanych na taśmach.

Operacje równoległe

Program Acronis Backup & Recovery 11 umożliwia równoczesne wykonywanie wielu operacji dotyczących różnych komponentów urządzenia taśmowego. Podczas operacji z użyciem napędu (takiej jak tworzenie kopii zapasowej, odzyskiwanie, ponowne skanowanie (s. 204) lub kasowanie (s. 204)) można uruchomić operację wykorzystującą zmieniacz (przenoszenie (s. 203) taśmy do innego gniazda lub jej wysuwanie (s. 204)) i na odwrót. Jeśli biblioteka taśm składa się z dwóch lub więcej napędów, można także równoległe uruchomić operację korzystającą z jednego z napędów podczas operacji z innym napędem. Na przykład możliwe jest jednoczesne tworzenie kopii zapasowych lub odzyskiwanie na kilku komputerach z użyciem różnych napędów tej samej biblioteki taśm.

Operację wykrywania nowych urządzeń taśmowych (s. 200) można wykonywać równoległe z dowolną inną operacją. Podczas inwentaryzacji (s. 206) nie można wykonywać żadnej innej operacji oprócz wykrywania nowych urządzeń taśmowych.

Operacje, których nie można przeprowadzać równocześnie, są kolejgowane.

Ograniczenia

Korzystanie z urządzenia taśmowego podlega następującym ograniczeniom:

1. Nie jest możliwa konsolidacja (s. 380) kopii zapasowych zapisanych na taśmach. W wyniku tego ograniczenia użycie schematów tworzenia kopii zapasowych jest związane z pewnymi uwarunkowaniami (s. 193).
2. Nie jest możliwa deduplikacja (s. 376) kopii zapasowych zapisanych na taśmach.
3. Uproszczone nazewnictwo plików kopii zapasowych (s. 70) nie jest dostępne w przypadku kopii zapasowych zapisywanych na taśmach.
4. Jeśli odzyskiwanie wymaga ponownego uruchomienia systemu operacyjnego, operacji odzyskiwania kopii zapasowej zapisanej na taśmach nie można przeprowadzić pod kontrolą tego systemu. Do tego celu należy użyć nośnika startowego.
5. Nie można odzyskiwać poszczególnych plików z kopii zapasowej na poziomie dysku przechowywanej na taśmach. Z tego powodu wykaz danych (s. 388) nie wyświetla plików i folderów zawartych w kopiach zapasowych na poziomie dysku.

6. Można sprawdzić poprawność (s. 231) dowolnej kopii zapasowej lub archiwum przechowywanego na taśmie, ale nie można wybrać do sprawdzenia poprawności całego skarbca taśmowego ani urządzenia taśmowego.
7. Skarbcza taśmowego nie można dołączać (s. 184) ani odłączać.
8. Zarządzanego skarbca taśmowego nie można zabezpieczyć za pomocą szyfrowania. Zamiast tego należy zaszyfrować poszczególne archiwa.
9. Nie jest możliwe utworzenie zarządzanego skarbca taśmowego (s. 179) z właściwością kompatybilności wstecz. Oznacza to, że agenty Acronis Backup & Recovery 10 nie mogą tworzyć kopii zapasowych w zarządzanych skarbcach taśmowych programu Acronis Backup & Recovery 11.
10. Program nie może jednocześnie zapisywać jednej kopii zapasowej na wielu taśmach ani wielu kopii zapasowych na jednej taśmie za pomocą tego samego napędu taśmowego.
11. Nie są obsługiwane urządzenia korzystające z protokołu NDMP.
12. Nie są obsługiwane drukarki kodów kreskowych.

Możliwość odczytu taśm zapisanych przez starsze wersje programów Acronis

W poniższej tabeli zestawiono możliwości odczytu w programie Acronis Backup & Recovery 11 taśm zapisanych przez produkty z rodzin Acronis True Image Echo, Acronis True Image 9.1 oraz Acronis Backup & Recovery 10. Tabela przedstawia również kompatybilność taśm zapisanych przez różne komponenty programu Acronis Backup & Recovery 11.

			...można odczytać przy użyciu urządzenia taśmowego podłączonego do komputera zawierającego...			
			Nośnik startowy ABR11	ABR11 Agent for Windows	ABR11 Agent for Linux	ABR11 Storage Node
Taśmę zapisaną na lokalnie podłączonym urządzeniu taśmowym (napędzie taśmowym lub w bibliotece taśm) przez...	Nośnik startowy	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11	+	+	+	+
	Agent dla systemu Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11	+	+	+	+
	Agent dla systemu Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11	+	+	+	+
Taśma zapisana na urządzeniu taśmowym przez...	Backup Server	9.1	-	-	-	-
		Echo	-	-	-	-
	Węzeł magazynowania	ABR10	+	+	+	+
		ABR11	+	+	+	+

6.3.3 Rozpoczęcie pracy z urządzeniem taśmowym

Tworzenie kopii zapasowej komputera na bezpośrednio podłączonym urządzeniu taśmowym

Wymagania wstępne

- Urządzenie taśmowe jest podłączone do komputera zgodnie z instrukcjami producenta.

- Na komputerze jest zainstalowany agent Acronis Backup & Recovery 11.

Przed utworzeniem kopii zapasowej

1. Włóż taśmy do urządzenia taśmowego.
2. Podłącz konsolę do komputera.
3. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**.
4. Kliknij **Wykryj urządzenia taśmowe**.
5. Jeśli urządzenie ma postać autonomicznego napędu, pomiń ten krok. W przeciwnym przypadku, wykonaj następujące czynności:

- a. Kliknij **Inwentaryzacja** w celu wykrycia taśm załadowanych. Wybierz metodę inwentaryzacji **Pełna**. Nie zaznaczaj pola wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.

Rezultat. Włożone taśmy zostały przeniesione do odpowiednich pul zgodnie z opisem w sekcji „Inwentaryzacja” (s. 206).

Pełna inwentaryzacja całego urządzenia taśmowego może zabrać dużo czasu.

- b. Jeśli załadowane taśmy zostały przesłane do puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy**, a chcesz je wykorzystać do tworzenia kopii zapasowych, przenieś (s. 203) je ręcznie do puli **Wolne taśmy**.

*Taśmy przesłane do puli **Zaimportowane taśmy** zawierają kopie zapasowe zapisane przez oprogramowanie Acronis. Przed ich przeniesieniem do puli **Wolne taśmy** upewnij się, że nie potrzebujesz już zapisanych na nich kopii zapasowych.*

Tworzenie kopii zapasowej

Z menu **Czynności** wybierz **Utwórz kopię zapasową** lub **Utwórz plan tworzenia kopii zapasowych**. Skonfiguruj (s. 48) ustawienia kopii zapasowej. Wybierz urządzenie taśmowe jako miejsce docelowe kopii zapasowej.

Rezultaty

- Powstałe kopie zapasowe zostaną umieszczone w automatycznie utworzonym skarbcu osobistym (s. 208). Aby uzyskać do niego dostęp, w drzewie **Nawigacja** kliknij **Skarbcze**. Po każdorazowym wybraniu urządzenia taśmowego jako miejsca docelowego kopii zapasowej tworzone kopie będą zapisywane w tym samym skarbcu.
- Taśmy z kopiami zapasowymi zostaną przeniesione do puli **Acronis**.

Tworzenie kopii zapasowej na urządzeniu taśmowym podłączonym do węzła magazynowania

Wymagania wstępne

- Węzeł magazynowania Acronis Backup & Recovery 11 Storage Node jest dodany do serwera zarządzania (s. 216).
- Urządzenie taśmowe jest podłączone do węzła magazynowania zgodnie z instrukcjami producenta.

Przed utworzeniem kopii zapasowej

1. Włóż taśmy do urządzenia taśmowego.
2. Podłącz konsolę do serwera zarządzania.
3. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Wybierz węzeł magazynowania, do którego jest podłączone urządzenie taśmowe.

4. Kliknij **Wykryj urządzenia taśmowe**.
5. Jeśli urządzenie ma postać autonomicznego napędu, pomiń ten krok. W przeciwnym przypadku, wykonaj następujące czynności:
 - a. Kliknij **Inwentaryzacja** w celu wykrycia taśm załadowanych. Wybierz metodę inwentaryzacji **Pełna**. Nie zaznaczaj pola wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.

Rezultat. Włożone taśmy zostały przeniesione do odpowiednich pul zgodnie z opisem w sekcji „Inwentaryzacja” (s. 206).

Pełna inwentaryzacja całego urządzenia taśmowego może zabrać dużo czasu.
 - b. Jeśli załadowane taśmy zostały przesłane do puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy**, a chcesz je wykorzystać do tworzenia kopii zapasowych, przenieś (s. 203) je ręcznie do puli **Wolne taśmy**.

*Taśmy przesłane do puli **Zaimportowane taśmy** zawierają kopie zapasowe zapisane przez oprogramowanie Acronis. Przed ich przeniesieniem do puli **Wolne taśmy** upewnij się, że nie potrzebujesz już zapisanych na nich kopii zapasowych.*

 - c. Zdecyduj, czy chcesz tworzyć kopie zapasowe w domyślnej puli Acronis (s. 200) czy wolisz utworzyć nową pulę (s. 201).

Informacje szczegółowe. Posiadanie kilku pul umożliwia używanie osobnego zestawu taśm dla każdego komputera lub działu w firmie. Użycie wielu pul zapobiega wymieszaniu na jednej taśmie kopii zapasowych utworzonych za pomocą różnych planów tworzenia kopii.
 - d. Jeśli jest wybrana pula **Acronis** lub nowa pula może w razie potrzeby pobierać taśmy z puli **Wolne taśmy**, pomiń ten krok.

W przeciwnym razie przenieś taśmy z puli **Wolne taśmy** do nowej puli.

Wskazówka. Aby dowiedzieć się, czy pula może pobierać taśmy z puli **Wolne taśmy**, kliknij pulę, a następnie kliknij **Szczegóły**.
6. W drzewie **Nawigacja** kliknij **Węzły magazynowania**. Wybierz węzeł magazynowania, do którego podłączone jest urządzenie taśmowe, a następnie kliknij **Utwórz skarbiec**. Przejdź do czynności opisanych w sekcji „Tworzenie zarządzanego skarbca centralnego (s. 179)”. W kroku **Pula taśm** wybierz pulę, która została wskazana w kroku 5c.

Jeśli urządzenie taśmowe jest podłączone do węzła magazynowania, konieczne jest utworzenie skarbcu centralnego.

Tworzenie kopii zapasowej

Z menu **Czynności** wybierz **Utwórz kopię zapasową** lub **Utwórz plan tworzenia kopii zapasowych**. Skonfiguruj (s. 315) ustawienia kopii zapasowych dla jednego lub więcej komputerów. Wybierz utworzony skarbiec jako miejsce docelowe kopii zapasowej.

Rezultaty

- Wynikowe kopie zapasowe zostaną umieszczone w utworzonym skarbcu.

Wskazówki dotyczące dalszego użycia biblioteki taśm

- Nie trzeba przeprowadzać pełnej inwentaryzacji przy każdym ładowaniu nowej taśmy. W celu zaoszczędzenia czasu postępuj zgodnie z procedurą opisaną w sekcji „Inwentaryzacja” (s. 206) w rozdziale „Połączenie szybkiej i pełnej inwentaryzacji”.
- W tej samej bibliotece taśm można również utworzyć inne skarbcie (s. 208) i wybrać dowolny z nich jako miejsce docelowe kopii zapasowych.

Odzyskiwanie z urządzenia taśmowego pod kontrolą systemu operacyjnego

Aby odzyskiwać dane z urządzenia taśmowego pod kontrolą systemu operacyjnego:

1. Podłącz konsolę do komputera, który chcesz odzyskać.
2. W menu **Czynności** kliknij **Odzyskaj**.
3. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
4. Wybierz skarbiec zawierający kopię zapasową z danymi, które chcesz odzyskać, i kliknij **Widok archiwum**.
5. Wybierz kopię zapasową, a następnie wybierz dane, które chcesz odzyskać. Po kliknięciu **OK** na stronie **Odzyskaj** zostanie wyświetlona lista taśm wymaganych do przeprowadzenia odzyskiwania. Brakujące taśmy są wyszarzone. Jeśli urządzenie taśmowe ma puste gniazda, włóż te taśmy do urządzenia.
6. Skonfiguruj (s. 130) inne ustawienia odzyskiwania.
7. Kliknij **OK**, aby rozpocząć operację odzyskiwania.
8. Jeśli którakolwiek z wymaganych taśm z jakiegoś powodu nie została włożona, program wyświetli komunikat z identyfikatorem wymaganej taśmy. Aby kontynuować odzyskiwanie, włóż taśmę i kliknij **Ponów**.

Co zrobić, jeśli nie widać kopii zapasowych przechowywanych na taśmach?

Może to oznaczać, że baza danych z zawartością taśm z jakiegoś powodu została utracona lub jest uszkodzona.

Aby odzyskać bazę danych, wykonaj następujące czynności:

Jeśli kopia zapasowa znajduje się na komputerze

1. Kliknij **Odzyskaj**, **Wybierz dane** i **Przeglądaj**.
2. Kliknij dwukrotnie **Urządzenia taśmowe**. System wyświetli monit o potwierdzenie wykrywania urządzeń taśmowych. Kliknij **Tak**.
3. Po pojawieniu się wykrytych urządzeń taśmowych w drzewie wybierz wymagane urządzenie i kliknij **OK**. System wyświetli monit o potwierdzenie operacji ponownego skanowania. Kliknij **Tak**.
4. Ponowne skanowanie (s. 204) puli **Nierozpoznane taśmy**. W jego wyniku odzyskasz zawartość włożonych taśm.
5. Jeśli którakolwiek z wykrytych kopii zapasowych jest kontynuowana na innych taśmach, które nie zostały jeszcze ponownie przeskanowane, po ukazaniu się monitu włóż te taśmy i przeskanuj je ponownie.
6. Po wykonaniu tych czynności można wybrać wymaganą kopię zapasową.

Jeśli kopia zapasowa znajduje się w węźle magazynowania

1. Podłącz konsolę do serwera zarządzania.
2. Wykryj urządzenia taśmowe (s. 200).
3. Przeprowadź szybką inwentaryzację (s. 206).

*Podczas inwentaryzacji nie zaznaczaj pola wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**. Zaznaczenie tego pola wyboru może spowodować utratę wszystkich kopii zapasowych.*

4. W urządzeniu taśmowym utwórz skarbiec (s. 208) zarządzany.
5. Ponowne skanowanie (s. 204) puli **Nierozpoznane taśmy**. W jego wyniku odzyskasz zawartość włożonych taśm.

6. Jeśli którakolwiek z wykrytych kopii zapasowych jest kontynuowana na innych taśmach, które nie zostały jeszcze ponownie przeskanowane, po ukazaniu się monitu włóż te taśmy i przeskanuj je ponownie.

Odzyskiwanie pod kontrolą nośnika startowego z lokalnie dołączonego urządzenia taśmowego

Aby odzyskać system pod kontrolą nośnika startowego z lokalnie dołączonego urządzenia taśmowego:

1. Włóż do urządzenia taśmowego taśmy wymagane do przeprowadzenia odzyskiwania.
2. Uruchom komputer za pomocą nośnika startowego.
3. Kliknij **Acronis Backup & Recovery 11**, a następnie kliknij **Zarządzaj tym komputerem lokalnie**. Pomiń ten krok, jeśli używasz nośnika opartego na środowisku WinPE.
4. Kliknij **Odzyskaj**.
5. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
6. Kliknij dwukrotnie **Urządzenia taśmowe**. System wyświetli monit o potwierdzenie wykrywania urządzeń taśmowych. Kliknij **Tak**.
7. Po tym, jak wykryte urządzenia taśmowe pojawią się w drzewie, wybierz wymagane urządzenie. System wyświetli monit o potwierdzenie ponownego skanowania. Kliknij **Tak**.
8. Wybierz pulę **Nierozpoznane taśmy**.
9. Wybierz taśmy do ponownego skanowania. Aby wybrać wszystkie taśmy z puli, zaznacz pole wyboru obok nagłówka kolumny **Nazwa taśmy**.
10. Jeśli taśmy zawierają archiwum zabezpieczone hasłem, określ hasło do archiwum w polu **Hasło**. Jeśli nie wprowadzisz hasła albo wprowadzisz niepoprawne hasło, archiwum nie zostanie wykryte. Pamiętaj o tym w przypadku braku archiwów po ponownym skanowaniu.
Wskazówka. Jeśli taśmy zawierają kilka archiwów zabezpieczonych różnymi hasłami, trzeba kilkakrotnie powtórzyć ponowne skanowanie, za każdym razem określając odpowiednie hasło.
11. Kliknij **Uruchom**, aby uruchomić ponowne skanowanie. W jego wyniku odzyskasz zawartość włożonych taśm.
12. Jeśli którakolwiek z wykrytych kopii zapasowych jest kontynuowana na innych taśmach, które nie zostały jeszcze ponownie przeskanowane, po ukazaniu się monitu włóż te taśmy i przeskanuj je ponownie.
13. W **Widoku archiwum** wybierz kopię zapasową, której dane chcesz odzyskać, a następnie wybierz dane do odzyskania. Po kliknięciu **OK** na stronie **Odzyskaj** zostanie wyświetlona lista taśm wymaganych do przeprowadzenia odzyskiwania. Brakujące taśmy są wyszarzone. Jeśli urządzenie taśmowe ma puste gniazda, włóż te taśmy do urządzenia.
14. Skonfiguruj (s. 130) inne ustawienia odzyskiwania.
15. Kliknij **OK**, aby rozpocząć odzyskiwanie.
16. Jeśli którakolwiek z wymaganych taśm z jakiegoś powodu nie została włożona, program wyświetli komunikat z identyfikatorem wymaganej taśmy. Aby kontynuować odzyskiwanie, włóż taśmę i kliknij **Ponów**.

Odzyskiwanie danych za pomocą nośnika startowego z urządzenia taśmowego dołączonego do węzła magazynowania

Aby odzyskać dane za pomocą nośnika startowego z urządzenia taśmowego dołączonego do węzła magazynowania:

1. Włóż do urządzenia taśmowego taśmy wymagane do przeprowadzenia odzyskiwania.
2. Uruchom komputer za pomocą nośnika startowego.

3. Kliknij **Acronis Backup & Recovery 11**, a następnie kliknij **Zarządzaj tym komputerem lokalnie**. Pomiń ten krok, jeśli używasz nośnika opartego na środowisku WinPE.
4. Kliknij **Odzyskaj**.
5. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
6. W polu **Ścieżka** wpisz `bsp://<adres węzła magazynowania>/<nazwa skarbca>/`, gdzie `<adres węzła magazynowania>` to adres IP węzła magazynowania zawierającego wymaganą kopię zapasową, a `<nazwa skarbca>` to nazwa skarbca. Kliknij **OK** i określ poświadczenia skarbca.
7. Wybierz kopię zapasową, a następnie wybierz dane, które chcesz odzyskać. Po kliknięciu **OK** na stronie **Odzyskaj** zostanie wyświetlona lista taśm wymaganych do przeprowadzenia odzyskiwania. Brakujące taśmy są wyszarzone. Jeśli urządzenie taśmowe ma puste gniazda, włóż te taśmy do urządzenia.
8. Skonfiguruj (s. 130) inne ustawienia odzyskiwania.
9. Kliknij **OK**, aby rozpocząć odzyskiwanie.
10. Jeśli którakolwiek z wymaganych taśm z jakiegoś powodu nie została włożona, program wyświetli komunikat z identyfikatorem wymaganej taśmy. Aby kontynuować odzyskiwanie, włóż taśmę i kliknij **Ponów**.

6.3.4 Zarządzanie taśmami

Wykrywanie urządzeń taśmowych

W trakcie procedury wykrywania urządzeń taśmowych program Acronis Backup & Recovery 11 znajduje wszystkie urządzenia taśmowe podłączone do komputera i umieszcza związane z nimi informacje w bazie danych zarządzania taśmami. Wykrywanie urządzeń taśmowych jest wymagane:

- Po podłączeniu lub ponownym podłączeniu urządzenia taśmowego.
- Po zainstalowaniu lub ponownym zainstalowaniu programu Acronis Backup & Recovery 11 na komputerze, do którego jest podłączone urządzenie taśmowe.

Po wykryciu urządzeń taśmowych program Acronis Backup & Recovery 11 uniemożliwia ich wykorzystanie przez menedżera RSM.

Aby wykryć urządzenia taśmowe

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij **Wykryj urządzenia taśmowe**. Zostaną wyświetlone informacje o liczbie podłączonych urządzeń taśmowych, ich napędów i gniazd.

Pule taśm

Program Acronis Backup & Recovery 11 korzysta z pul taśm będących logicznymi grupami taśm. Program zawiera następujące wstępnie zdefiniowane pule taśm: **Nierozpoznane taśmy**, **Zaimportowane taśmy**, **Wolne taśmy** oraz **Acronis**. Można również tworzyć własne, niestandardowe pule.

Wstępnie zdefiniowane pule

Nierozpoznane taśmy

Pula zawiera taśmy, które były zapisane przez aplikacje innych firm. Aby móc na nich zapisywać, należy je jawnie przenieść (s. 203) do puli **Wolne taśmy**. Taśm z tej puli nie można przenosić do żadnej innej puli niż **Wolne taśmy**.

Zaimportowane taśmy

Pula zawiera taśmy zapisane przez program Acronis Backup & Recovery 11 na urządzeniu taśmowym dołączonym do innego węzła przechowywania lub agenta. Aby móc na nich zapisywać, należy je jawnie **przenieść** do puli Wolne taśmy. Taśm z tej puli nie można przenosić do żadnej innej puli niż **Wolne taśmy**.

Wolne taśmy

Pula zawiera wolne (puste) taśmy. Taśmy z tej puli można ręcznie przenosić do innych pul.

W przypadku przenoszenia taśmy do puli **Wolne taśmy** oprogramowanie oznaczy ją jako pustą. Jeśli taśma zawiera kopie zapasowe, są one prezentowane jako usunięte. Zastępowanie kopii zapasowych wiąże się z usunięciem związanych z nimi danych z bazy danych.

Acronis

Pula służy domyślnie do tworzenia kopii zapasowych, jeśli użytkownik nie chce utworzyć własnych pul. Zwykle odnosi się ona do pojedynczego napędu z niewielką liczbą taśm.

Pule niestandardowe

Jeśli chcesz oddzielić kopie zapasowe różnych danych, musisz utworzyć kilka pul. Warto na przykład utworzyć niestandardowe pule w celu oddzielenia:

- kopii zapasowych pochodzących z poszczególnych działów firmy;
- kopii zapasowych poszczególnych komputerów;
- kopii zapasowych woluminów systemowych i danych użytkowników;
- taśm zapełnionych od taśm zapisywanych (s. 201).

Oddzielanie zapełnionych taśm

Czasem warto oddzielić taśmy zapełnione od niezapełnionych. Załóżmy, że taśmy obejmujące ponad miesiąc chcesz przenosić do innej lokalizacji. W tym celu:

1. Utwórz niestandardową pulę taśm (s. 201) (na przykład **Zapełnione taśmy**).
2. Utwórz kolejną pulę taśm (na przykład **Bieżące taśmy**). W ustawieniach puli zaznacz pole wyboru **Gdy taśma jest pełna, przenieś ją do puli**, a na liście zaznacz pulę **Zapełnione taśmy**.
3. Utwórz skarbiec (s. 208) i powiąż go z pulą **Bieżące taśmy**.
4. Tworząc plan tworzenia kopii zapasowych, wybierz utworzony skarbiec jako miejsce docelowe kopii zapasowych.
5. Raz w miesiącu wysuń taśmy przechowywane w puli **Zapełnione taśmy** i przenieś je do innej lokalizacji.

Operacje dotyczące pul

Tworzenie puli

Aby utworzyć pulę:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij **Nowa pula**.
3. Określ nazwę puli.

4. [Opcjonalnie] Z puli **Wolne taśmy** wybierz taśmy, które mają zostać przeniesione do tworzonej puli.
5. [Opcjonalnie] Usuń zaznaczenie pola wyboru **W razie potrzeby automatycznie pobieraj taśmy z puli wolnych taśm**. Jeśli pole to nie jest zaznaczone, do tworzenia kopii zapasowych będą użyte tylko te taśmy, które w określonym momencie znajdują się w nowej puli.
6. [Opcjonalnie] Zaznacz pole wyboru **Po ... ponownych zapisach przenieś taśmę do puli**, określ liczbę cykli zapisu informacji, a następnie wybierz pulę, do której taśma zostanie przeniesiona po upłynięciu danej liczby cykli.

Wskazówka. Taśmy są stosunkowo nietrwałe. Można więc utworzyć specjalną pulę i przenosić do niej stare taśmy. Następnie należy regularnie wysuwać taśmy przechowywane w tej puli, usuwać je i ładować do urządzenia nowe taśmy.

7. [Opcjonalnie] Zaznacz pole wyboru **Po ... kopiach zapasowych przenieś taśmę do puli**, określ liczbę kopii zapasowych, a następnie wybierz pulę, do której taśma zostanie przeniesiona po utworzeniu danej liczby kopii.

Wskazówka. Opcja ta może być przydatna na przykład w następującym przypadku. Codziennie od poniedziałku do piątku tworzysz kopie zapasowe komputera, a po utworzeniu pięciu kopii przenosisz taśmy do puli niestandardowej. Raz w tygodniu specjalnie wyznaczeni pracownicy wysuwają taśmy z tej puli i zabezpieczają je w innej lokalizacji.

8. [Opcjonalnie] Zaznacz pole wyboru **Gdy taśma jest pełna, przenieś ją do puli**, a następnie wybierz pulę, do której zostanie przeniesiona zapełniona taśma.

Wskazówka. Opcja ta może być przydatna na przykład do oddzielania taśm zapełnionych od zapisywanych (s. 201).

9. Kliknij **OK**.

Edycja puli

Program umożliwia edycję parametrów puli **Acronis** oraz pul niestandardowych.

Aby wyedytować pulę:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Wybierz żadaną pulę i kliknij **Ustawienia**.
3. Można zmienić nazwę puli (z wyjątkiem nazwy puli **Acronis**) lub jej ustawienia. Aby uzyskać więcej informacji o ustawieniach pul, zobacz „Tworzenie puli” (s. 201).
4. Kliknij **OK**, aby zapisać zmiany.

Usuwanie puli

Program umożliwia usuwanie tylko pul niestandardowych. Wstępnie zdefiniowanych pul taśm (**Nierozpoznane taśmy**, **Zaimportowane taśmy**, **Wolne taśmy** i puli **Acronis**) nie można usunąć.

Aby usunąć pulę:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Wybierz żadaną pulę i kliknij **Usuń**.
3. Wybierz pulę, do której zostaną przeniesione taśmy z usuwanej puli po jej usunięciu.
4. Kliknij **OK**, aby usunąć pulę.

Operacje na taśmach

Zmiana nazwy

Po wykryciu taśmy przez program jest jej automatycznie przypisywana nazwa w następującym formacie: **Taśma_XXX**, gdzie **XXX** to unikatowy numer. Jeśli urządzenie taśmowe jest wyposażone w czytnik kodów kreskowych, numer ten odpowiada kodowi kreskowemu taśmy. Jeśli urządzenie taśmowe nie jest wyposażone w czytnik kodów paskowych, taśmom są nadawane kolejne numery. Operacja zmiany nazwy umożliwia ręczną zmianę nazwy jednej lub kilku taśm.

Aby zmienić nazwy taśm:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij pulę zawierającą wymagane taśmy, a następnie wybierz żądane taśmy.
3. Kliknij **Zmień nazwę**.
4. Wpisz nowe nazwy wybranych taśm.
5. Kliknij **OK**, aby zapisać zmiany.

Zmiana puli

Ta operacja służy do przenoszenia jednej lub kilku taśm z jednej puli do drugiej.

W przypadku przenoszenia taśmy do puli **Wolne taśmy** oprogramowanie oznaczy ją jako pustą. Jeśli taśma zawiera kopie zapasowe, są one prezentowane jako usunięte. Zastępowanie kopii zapasowych wiąże się z usunięciem związanych z nimi danych z bazy danych.

Uwagi dotyczące określonych typów taśm

- Do puli **Wolne taśmy** nie można przenosić taśm zabezpieczonych przed zapisem ani taśm jednokrotnego zapisu WORM (ang. Write-Once-Read-Many).
- Taśmy czyszczące są zawsze wyświetlane w puli **Nierozpoznane taśmy** i nie można ich przenieść do innej puli.

Aby przenieść taśmy do innej puli:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij pulę zawierającą wymagane taśmy, a następnie wybierz żądane taśmy.
3. Kliknij **Zmień pulę**.
4. [Opcjonalnie] Kliknij **Nowa pula**, jeśli chcesz utworzyć kolejną pulę dla wybranych taśm. Wykonaj czynności opisane w sekcji „Tworzenie puli” (s. 201).
5. Wybierz pulę, do której chcesz przenieść taśmy.
6. Kliknij **OK**, aby zapisać zmiany.

Przenoszenie do innego gniazda

Zastosuj tę operację w następujących sytuacjach:

- Musisz wyjąć jednocześnie kilka taśm z urządzenia taśmowego.
- Urządzenie taśmowe nie jest wyposażone w gniazdo pocztu, a wyjmowane taśmy znajdują się w gniazdach magazynków niewymiennych.

Należy pojedynczo przenosić taśmy do gniazd jednego magazynka, a następnie ręcznie wyjąć magazynek.

Aby przenieść taśmę do innego gniazda:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij pulę zawierającą wymaganą taśmę, a następnie wybierz żadaną taśmę.
3. Kliknij **Przenieś**.
4. Wybierz nowe gniazdo, do którego chcesz przenieść wybraną taśmę.
5. Kliknij **OK**, aby rozpocząć operację.

Wysuwanie

Aby pomyślnie wysunąć taśmę z biblioteki taśm, biblioteka musi być wyposażona w gniazdo pocztu, które nie może być zablokowane przez użytkownika lub inne oprogramowanie.

Aby wysunąć taśmę:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij pulę zawierającą wymaganą taśmę, a następnie wybierz żadaną taśmę.
3. Kliknij **Wysuń**. Program wyświetli monit o podanie opisu taśmy. Zaleca się uwzględnienie w nim fizycznej lokalizacji, w której taśma będzie przechowywana. Program wyświetli ten opis w trakcie odzyskiwania, aby można było łatwo odnaleźć potrzebną taśmę.

Informacje szczegółowe. Monit o podanie opisu taśmy można wyłączyć, klikając **Nie wyświetlaj ponownie tego komunikatu**. Aby go ponownie włączyć: w menu kliknij **Opcje**, następnie **Opcje konsoli**, kliknij **Komunikaty wyskakujące**, a następnie zaznacz pole wyboru **Żądaj podania opisu podczas wysuwania taśmy**.

4. Kliknij **OK**, aby rozpocząć operację.

Po ręcznym lub automatycznym (s. 124) wysunięciu taśmy zaleca się umieszczenie na niej jej nazwy.

Kasowanie

Skasowanie zawartości taśmy powoduje fizyczne usunięcie wszystkich przechowywanych na niej kopii zapasowych oraz usunięcie informacji o tych kopiach z bazy danych. Informacja o samej taśmie pozostanie jednak w bazie danych.

Po skasowaniu taśma zlokalizowana w puli **Nierozpoznane taśmy** lub w puli **Zaimportowane taśmy**, jest przenoszona do puli **Wolne taśmy**. Taśmy z innych pul nie będą przenoszone.

Operację można jednocześnie zastosować w odniesieniu do pojedynczej taśmy.

Aby skasować taśmę:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij pulę zawierającą wymaganą taśmę, a następnie wybierz żadaną taśmę.
3. Kliknij **Kasuj**. System wyświetli monit z prośbą o potwierdzenie operacji.
4. Kliknij **OK**, aby rozpocząć operację.

Ponowne skanowanie

Informacje o zawartości taśm są przechowywane w specjalnej bazie danych. Operacja ponownego skanowania powoduje odczyt zawartości taśm i aktualizację bazy danych, jeśli informacje w niej nie

odpowiadają danym przechowywanym na taśmach. Archiwa wykryte w wyniku tej operacji są umieszczane w określonym skarbku.

W czasie jednej operacji można ponownie skanować taśmy z jednej puli. Operacja jest możliwa tylko w odniesieniu do taśm w trybie online.

Uruchom ponowne skanowanie:

- Jeśli baza danych węzła magazynowania lub komputera zarządzanego została utracona lub uległa uszkodzeniu.
- Jeśli informacje o taśmie zapisane w bazie danych są nieaktualne (zawartość taśmy została na przykład zmodyfikowana przez innego agenta lub węzeł magazynowania).
- Aby uzyskać dostęp do kopii zapasowych przechowywanych na taśmach z poziomu nośnika startowego.
- Jeśli przypadkowo usunięto (s. 207) z bazy danych informacje na temat taśmy. Po ponownym przeskanowaniu usuniętej taśmy przechowywane na niej kopie zapasowe znów pojawią się w bazie danych i staną się dostępne do odzyskania.
- Jeśli kopie zapasowe zostały usunięte z taśmy ręcznie lub za pośrednictwem reguł przechowywania (s. 383), ale chcesz je udostępnić do operacji odzyskiwania danych. Przed ponownym skanowaniem takiej taśmy, wysuń (s. 204) ją, usuń (s. 207) z bazy danych informacje jej dotyczące, a następnie ponownie włóż taśmę do urządzenia taśmowego.

Aby ponownie przeskanować taśmy:

1. Jeśli nie dysponujesz skarbkiem taśmowym (s. 208) powiązany z urządzeniem, do którego załadowano taśmy, utwórz go.
2. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
3. Przeprowadź szybką inwentaryzację (s. 206).

*Podczas inwentaryzacji nie zaznaczaj pola wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.*

4. Kliknij **Skanuj ponownie**.
5. Wybierz skarbiec, w którym zostaną umieszczone nowo wykryte archiwa.
6. Wybierz pulę **Nierozpoznane taśmy**. Jest to pula, do której wysyłana jest większość taśm nagranych w wyniku szybkiej inwentaryzacji. Możliwe jest także ponowne skanowanie puli skojarzonej z wybranym skarbkiem lub puli **Zaimportowane taśmy**.
7. Wybierz taśmy do ponownego skanowania. Aby wybrać wszystkie taśmy z puli, zaznacz pole wyboru obok nagłówka kolumny **Nazwa taśmy**.
8. Jeśli taśmy zawierają archiwum zabezpieczone hasłem, określ hasło do archiwum w polu **Hasło**. Jeśli nie wprowadzisz hasła albo wprowadzisz niepoprawne hasło, archiwum nie zostanie wykryte. Pamiętaj o tym w przypadku braku archiwów po ponownym skanowaniu.

Wskazówka. Jeśli taśmy zawierają kilka archiwów zabezpieczonych różnymi hasłami, trzeba kilkakrotnie powtórzyć ponowne skanowanie, za każdym razem określając odpowiednie hasło.

9. Kliknij **Uruchom**, aby uruchomić ponowne skanowanie.

Rezultat. Wybrane taśmy zostały przeniesione do puli powiązanej z wybranym skarbkiem. Zawiera on kopie zapasowe przechowywane na tych taśmach. Kopia zapasowa znajdująca się na kilku taśmach nie pojawi się w skarbku, dopóki wszystkie taśmy kopii zapasowej nie zostaną ponownie przeskanowane.

Inwentaryzacja

Operacja inwentaryzacji wykrywa taśmy załadowane w urządzeniu taśmowym i przypisuje nazwy jeszcze nienazwanym taśmom. Wykonaj tę operację, ilekroć ładujesz taśmy do gniazd urządzenia.

Metody inwentaryzacji

Program Acronis Backup & Recovery 11 dysponuje dwiema metodami inwentaryzacji.

Szybka inwentaryzacja

Program Acronis Backup & Recovery 11 skanuje taśmy w poszukiwaniu kodów kreskowych. Dzięki stosowaniu kodów kreskowych oprogramowanie może szybko zwrócić taśmę do puli, z której ona pochodzi.

Ta metoda umożliwia rozpoznawanie taśm używanych przez to samo urządzenie taśmowe podłączone do tego samego komputera. Inne taśmy zostaną wysłane do puli **Nierozpoznane taśmy**.

Jeśli biblioteka taśm nie jest wyposażona w czytnik kodów kreskowych, wszystkie taśmy zostaną wysłane do puli **Nierozpoznane taśmy**. W celu rozpoznania taśm należy przeprowadzić pełną inwentaryzację lub zastosować połączenie szybkiej i pełnej inwentaryzacji w sposób opisany poniżej.

Pełna inwentaryzacja

Program Acronis Backup & Recovery 11 odczytuje znaczniki zapisane przez oprogramowanie firmy Acronis i analizuje inne informacje o zawartości załadowanych taśm. Ta metoda umożliwia rozpoznawanie pustych taśm oraz taśm zapisanych przez oprogramowanie firmy Acronis w każdym urządzeniu taśmowym i na każdym komputerze.

W poniższej tabeli znajdują się pule, do których w wyniku pełnej inwentaryzacji są wysyłane taśmy.

Taśma była używana przez...	Taśma jest odczytywana przez...	Taśma jest wysyłana do puli...
agenta	tego samego agenta	w której znajdowała się wcześniej
	innego agenta	Zaimportowane taśmy
	Węzeł magazynowania	Zaimportowane taśmy
Węzeł magazynowania	ten sam węzeł magazynowania	w której znajdowała się wcześniej
	inny węzeł magazynowania	Zaimportowane taśmy
	agenta	Zaimportowane taśmy
aplikację do tworzenia kopii zapasowych innej firmy	agenta lub węzeł magazynowania	Nierozpoznane taśmy

Taśmy pewnych typów są wysyłane do określonych pul:

Typ taśmy	Taśma jest wysyłana do puli...
Pusta taśma	Wolne taśmy
Pusta taśma zabezpieczona przed zapisem	Nierozpoznane taśmy
Taśma czyszcząca	Nierozpoznane taśmy

Szybka inwentaryzację można stosować do całych urządzeń taśmowych. Pełną inwentaryzację można stosować do całych urządzeń taśmowych, pojedynczych napędów oraz gniazd.

Połączenie szybkiej i pełnej inwentaryzacji

Pełna inwentaryzacja całego urządzenia taśmowego może zabrać dużo czasu. Jeśli zinwentaryzowania wymaga tylko kilka taśm, wykonaj następujące czynności:

1. Przeprowadź szybką inwentaryzację urządzenia taśmowego.
2. Kliknij pulę **Nierozpoznane taśmy**. Znajdź taśmy do inwentaryzacji i zapisz, które gniazda one zajmują.
3. Przeprowadź pełną inwentaryzację tych gniazd.

Co zrobić po inwentaryzacji

Jeśli chcesz tworzyć kopie zapasowe na taśmach znajdujących się w puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy**, przenieś (s. 203) je do puli **Wolne taśmy**, a następnie do puli **Acronis** lub puli niestandardowej. Jeśli pula, w której chcesz tworzyć kopie zapasowe, jest uzupełnialna (s. 383), możesz pozostawić taśmy w puli **Wolne taśmy**.

Jeśli chcesz odzyskać dane z taśmy znajdującej się w puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy**, musisz ją ponownie przeskanować (s. 204). Taśma zostanie przeniesiona do puli powiązanej ze skarbcom wybranym podczas ponownego skanowania, a kopie zapasowe przechowywane na taśmie pojawią się w tym skarbcu.

Kolejność czynności

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij **Inwentaryzacja**.
3. Wybierz metodę inwentaryzacji: **Szybka** lub **Pełna**.
4. [Opcjonalnie] Zaznacz pole wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.

Ostrzeżenie. Zaznacz to pole wyboru, jeśli masz absolutną pewność, że dane przechowywane na taśmach nie będą więcej potrzebne i mogą zostać zastąpione.

5. [Opcjonalnie] Wybierz biblioteki taśm i napędy autonomiczne przeznaczone do inwentaryzacji. Domyślnie wybrane są wszystkie biblioteki taśm i napędy autonomiczne.
6. [Opcjonalnie] Jeśli wybierzesz inwentaryzację **pełną**, możesz wybrać gniazda, które mają być nią objęte. Domyślnie wybrane są wszystkie gniazda.

Usuwanie

Operacja usuwania usuwa z bazy danych informacje na temat kopii zapasowych przechowywanych na wybranej taśmie oraz dotyczące samej taśmy.

Usuwać można tylko taśmy w trybie offline (wysunięte (s. 204)).

Aby usunąć taśmę:

1. W drzewie **Nawigacja** kliknij **Zarządzanie taśmami**. Jeśli program jest połączony z serwerem zarządzania, wybierz węzeł magazynowania, do którego jest dołączone urządzenie taśmowe.
2. Kliknij pulę zawierającą wymaganą taśmę, a następnie wybierz żadaną taśmę.
3. Kliknij **Usuń**. System wyświetli monit z prośbą o potwierdzenie operacji.
4. Kliknij **OK**, aby usunąć taśmę.

Co zrobić w przypadku przypadkowego usunięcia taśmy?

W odróżnieniu od taśmy skasowanej (s. 204) dane z taśmy usuniętej nie są fizycznie usuwane. Z tego względu kopie zapasowe przechowywane na takiej taśmie można ponownie udostępnić. W tym celu:

1. Załaduj taśmę do urządzenia taśmowego.
2. Przeprowadź szybką inwentaryzację (s. 206) w celu wykrycia taśmy.

*Podczas inwentaryzacji nie zaznaczaj pola wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.*

3. Wykonaj ponowne skanowanie (s. 204), aby dopasować dane przechowywane na taśmach do informacji w bazie danych.

6.3.5 Skarbce na taśmach

Każdy skarbiec taśmowy jest powiązany z jednym lub kilkoma napędami urządzenia taśmowego oraz z pulą (s. 200) taśm.

Do czego potrzebnych jest kilka skarbców?

Poniżej przytoczono dwa z najczęstszych scenariuszy wymagających utworzenia kilku skarbców:

- Chcesz tworzyć kopie zapasowe danych z kilku komputerów, tak aby kopie z każdego komputera znajdowały się na osobnym zestawie taśm.
- Chcesz tworzyć kopie zapasowe różnych danych z tego samego komputera na osobnych zestawach taśm. Chcesz na przykład co tydzień tworzyć kopię zapasową woluminu systemowego, a codziennie kopię często zmieniających się danych.

W każdym z tych przypadków należy utworzyć osobną pulę niestandardową dla każdego zestawu taśm oraz powiązać z nią osobny skarbiec.

Osobiste skarbce taśmowe

Przed utworzeniem na bezpośrednio podłączonym urządzeniu taśmowym kopii zapasowej komputera można utworzyć skarbiec osobisty. W przeciwnym razie program automatycznie utworzy skarbiec osobisty powiązany z pulą **Acronis**.

Jeśli utworzysz więcej niż jeden skarbiec osobisty, taśmy z kopiami zapasowymi zostaną umieszczone w odpowiednich pulach określonych w ustawieniach skarbca. Jednak każdy skarbiec będzie wyświetlać wszystkie kopie zapasowe znajdujące się we wszystkich skarbcach.

Aby utworzyć skarbiec osobisty:

1. W drzewie **Nawigacja** kliknij **Skarbce**.
2. Kliknij **Utwórz**.
3. Przejdź do czynności opisanych w sekcji „Tworzenie skarbca osobistego (s. 187)”.

Zarządzane centralne skarbce taśmowe

Aby utworzyć kopię zapasową komputera na urządzeniu taśmowym dołączonym do węzła magazynowania, musisz utworzyć na tym urządzeniu zarządzany skarbiec centralny.

Aby utworzyć zarządzany skarbiec centralny:

1. W drzewie **Nawigacja** kliknij **Węzły magazynowania**.
2. Wybierz żądany węzeł magazynowania i kliknij **Utwórz skarbiec**.
3. Przejdź do czynności opisanych w sekcji „Tworzenie zarządzanego skarbca centralnego (s. 179)”.

Wskazówka. Jeśli tworzysz kopie zapasowe wielu komputerów w bibliotece taśm wyposażonej w wiele napędów, powiąż skarbiec z całą biblioteką. Pozwoli to na jednoczesne tworzenie kopii zapasowych komputerów za pomocą poszczególnych napędów. Jeśli powiążesz jeden lub kilka skarbców z pojedynczym napędem, będą tworzone kolejki kopii zapasowych.

6.3.6 Przykłady użycia

W uzupełnieniu przykładów opisanych w tej sekcji można wziąć pod uwagę następujące dwa przykłady:

- Przenoszenie starszych kopii zapasowych na taśmy do długoterminowego przechowywania (s. 97) (dysk-dysk-taśma)
- Tworzenie kopii zapasowych na taśmach w krótkim czasie wyznaczonym na tworzenie kopii (s. 98)

Przykład 1. Zmieniacz taśm i 12 taśm

Rozważmy następujący scenariusz:

- Masz 12 taśm i zmieniacz dołączony do komputera, którego dane chcesz uwzględnić w kopii zapasowej.
- Chcesz utworzyć kopię zapasową danych komputera w taki sposób, aby w przypadku braku wystarczającej ilości wolnego miejsca na taśmie tworzenie kopii zapasowej było kontynuowane na kolejnej taśmie.
- Po zapełnieniu wszystkich taśm chcesz kolejno zastępować ich zawartość bez działania użytkownika.

Potrzebna jest osobna pula dla planu tworzenia kopii zapasowych realizującego ten scenariusz. Jeśli masz lub zamierzasz utworzyć inne plany tworzenia kopii zapasowych zapisujące na tym samym urządzeniu taśmowym, użyj dla nich innych pul.

Kolejność czynności

1. Włóż taśmy do gniazd zmieniacza.
2. Wykonaj szybką inwentaryzację (s. 206) z zaznaczonym polem wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.
Rezultat. Załadowane taśmy znajdują się w puli **Wolne taśmy**. Jeśli część z nich znajduje się w puli **Acronis** lub w puli niestandardowej, oznacza to, że na taśmach znajdują się kopie zapasowe wcześniej utworzone na danym komputerze. Przenieś (s. 203) te taśmy ręcznie do puli **Wolne taśmy**, jeśli nie potrzebujesz już tych kopii zapasowych.
3. Zdecyduj, czy chcesz tworzyć kopie zapasowe w domyślnej puli **Acronis** (s. 200), czy wolisz utworzyć nową pulę (s. 201). W obu przypadkach wyczyść pole wyboru **W razie potrzeby automatycznie pobieraj taśmy z puli wolnych taśm** w ustawieniach wybranej puli.
4. Przenieś wszystkie załadowane taśmy z puli **Wolne taśmy** do puli wybranej.
5. Utwórz skarbiec (s. 208) osobisty i powiąż z nim pulę.
6. Podczas tworzenia planu tworzenia kopii zapasowych (s. 48):
 - Wybierz skarbiec jako lokalizację kopii zapasowych.
 - Wybierz **Niestandardowy** schemat tworzenia kopii zapasowych. Tak ustaw harmonogramy tworzenia kopii zapasowych, aby cały zestaw 12 taśm zawierał przynajmniej dwie pełne kopie zapasowe. Pozwoli to programowi na zastępowanie zawartości taśm w razie potrzeby.
 - W polu **Czyszczenie archiwum** wybierz wartość **Gdy w trakcie tworzenia kopii zapasowej zabraknie miejsca**.

Rezultat

Plan tworzenia kopii zapasowych będzie używał tylko taśm z wybranej puli. Po zapełnieniu wszystkich taśm zostanie zastąpiona zawartość najstarszej z nich i tak dalej.

Przykład 2. Tworzenie kopii zapasowych na taśmach w cyklu tygodniowym

Rozważmy następujący scenariusz:

- Chcesz utworzyć kopie zapasowe kilku komputerów w urządzeniu taśmowym dołączonym do węzła magazynowania Acronis Backup & Recovery 11 Storage Node.
- Chcesz tworzyć pełne kopie zapasowe w piątki oraz kopie przyrostowe w poniedziałki, wtorki, środy i czwartki.
- Chcesz korzystać z dwóch zestawów taśm, z których każdy będzie zapisywany w ciągu tygodnia. Zestaw taśm z właśnie zakończonego tygodnia powinien być wysuwany i zastępowany drugim zestawem, którego zawartość zostanie z kolei zastąpiona później. Ten scenariusz pracy może być przydatny, jeśli liczba gniazd urządzenia taśmowego wystarcza tylko do tworzenia kopii zapasowych w ciągu tygodnia.

Kolejność czynności

1. Włóż jeden z zestawów taśm do gniazd urządzenia taśmowego.
2. Wykonaj szybką inwentaryzację (s. 206) z zaznaczonym polem wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.
Rezultat. Załadowane taśmy znajdują się w puli **Wolne taśmy**. Jeśli część z nich znajduje się w puli **Acronis** lub w puli niestandardowej, oznacza to, że na taśmach znajdują się kopie zapasowe wcześniej utworzone na danym komputerze. Przenieś (s. 203) te taśmy ręcznie do puli **Wolne taśmy**, jeśli nie potrzebujesz już tych kopii zapasowych.
3. Zdecyduj, czy chcesz tworzyć kopie zapasowe w domyślnej puli Acronis (s. 200), czy wolisz utworzyć nową pulę (s. 201).
4. Jeśli wybrana pula nie jest uzupełnialna (s. 383), przenieś do niej wszystkie załadowane taśmy z puli **Wolne taśmy**.
5. Wsuń zestaw załadowanych taśm. Powtórz kroki 1, 2 i 4 dla drugiego zestawu taśm.
6. Utwórz zarządzany skarbiec centralny (s. 179). Tworząc skarbiec:
 - W polu **Napędy** wybierz całe urządzenie taśmowe. Umożliwi to jednoczesne tworzenie kopii zapasowych komputerów za pomocą różnych napędów, jeśli urządzenie taśmowe jest wyposażone w więcej niż jeden napęd.
 - W polu **Pula taśm** wybierz pulę, w której będą tworzone kopie zapasowe (pulę **Acronis** lub nowo utworzoną pulę).
7. W razie tworzenia scentralizowanego planu tworzenia kopii zapasowych (s. 315):
 - W polu **Elementy uwzględniane w kopii zapasowej** wybierz komputery, które chcesz uwzględnić w kopiach zapasowych.
 - Wybierz utworzony skarbiec jako miejsce docelowe kopii zapasowych.
 - Wybierz **Niestandardowy** schemat tworzenia kopii zapasowych.
 - Określ harmonogramy pełnych i przyrostowych kopii zapasowych.
 - W polu **Czyszczenie archiwum** wybierz **Używanie reguł przechowywania**, a następnie kliknij **Reguły przechowywania**. Określ regułę przechowywania tak, aby powodowała usunięcie kopii starszych niż 1 tydzień.

8. W każdy piątek, przed utworzeniem pełnej kopii zapasowej, wysuń włożony zestaw taśm i włóż drugi zestaw. Jeśli urządzenie taśmowe jest wyposażone w czytnik kodów kreskowych, wykonaj szybką inwentaryzację. W przeciwnym razie wykonaj pełną inwentaryzację.

Rezultat

Zestawy taśm będą używane naprzemiennie. Po włożeniu zestawu taśm zawartość jego taśm będzie kolejno zastępowana.

Przykład 3. Przenoszenie danych „z dysku na dysk na taśmę” z wysyłaniem taśm do magazynu w innej lokalizacji.

Rozważmy następujący scenariusz:

- Chcesz utworzyć kopię zapasową komputera na dysku twardym i replikować każdą kopię zapasową na urządzenie taśmowe podłączone do komputera lokalnego.
- Chcesz wysunąć taśmy z każdą kopią zapasową i wysłać je do innej lokalizacji.

Kolejność czynności

1. Wsuń taśmy do gniazd urządzenia taśmowego.
2. Wykonaj szybką inwentaryzację (s. 206) z zaznaczonym polem wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.
Rezultat. Załadowane taśmy znajdują się w puli **Wolne taśmy**. Jeśli część z nich znajduje się w puli **Acronis** lub w puli niestandardowej, oznacza to, że na taśmach znajdują się kopie zapasowe wcześniej utworzone na danym komputerze. Przenieś (s. 203) te taśmy ręcznie do puli **Wolne taśmy**, jeśli nie potrzebujesz już tych kopii zapasowych.
3. Zdecyduj, czy chcesz tworzyć kopie zapasowe w domyślnej puli **Acronis** (s. 200) czy wolisz utworzyć nową pulę (s. 201).
4. Jeśli wybrana pula nie jest uzupełnialna (s. 383), przenieś do niej wszystkie załadowane taśmy z puli **Wolne taśmy**.
5. Utwórz skarbiec (s. 208) osobisty i powiąż z nim pulę.
6. Podczas tworzenia planu tworzenia kopii zapasowych (s. 48):
 - Wybierz folder lokalny jako miejsce docelowe kopii zapasowych.
 - Ustaw wymagany schemat tworzenia kopii zapasowych.
 - Kliknij **Pokaż typ kopii zapasowej, Druga lokalizacja...**, zaznacz pole wyboru **Replikuj nowo utworzoną kopię zapasową do innej lokalizacji**, kliknij **Druga lokalizacja** i wybierz z drzewa utworzony skarbiec.
 - Kliknij **Opcje tworzenia kopii zapasowych**, kliknij **Zarządzanie taśmami** (s. 124) w drzewie, a następnie zaznacz pole wyboru **Wysuń taśmę**.
7. Po utworzeniu wszystkich kopii zapasowych i wysunięciu zawierających je taśm można wysłać taśmy do bezpiecznego magazynu w innej lokalizacji. Jeśli nie masz dostatecznej liczby wolnych taśm, aby kontynuować tworzenie kopii zapasowych, załaduj nowe taśmy i wykonaj kroki 2 i 4.

Rezultat

W lokalnym folderze i na taśmach zostanie utworzona kopia zapasowa komputera. Taśmy zawierające wszystkie kopie zapasowe zostaną wysłane do magazynu w innej lokalizacji.

Przykład 4. Dziadek-ojciec-syn. Wysyłanie pełnych kopii zapasowych do innej lokalizacji

Rozważmy następujący scenariusz:

- Chcesz tworzyć kopię zapasową komputera w urządzeniu taśmowym dołączonym do węzła magazynowania.
- Chcesz zastosować schemat tworzenia kopii zapasowych Dziadek-ojciec-syn (s. 56).
- Chcesz tworzyć pełne, przyrostowe i różnicowe kopie zapasowe. Każda pełna kopia zapasowa powinna być zapisywana na osobnej taśmie w celu wysłania jej do innej, bezpiecznej lokalizacji.

Kolejność czynności

1. Wsuń taśmy do gniazd urządzenia taśmowego.
2. Wykonaj szybką inwentaryzację (s. 206) z zaznaczonym polem wyboru **Przenieś nowo wykryte taśmy z puli „Nierozpoznane taśmy” lub „Zaimportowane taśmy” do puli „Wolne taśmy”**.
Rezultat. Załadowane taśmy znajdują się w puli **Wolne taśmy**. Jeśli część z nich znajduje się w puli **Acronis** lub w puli niestandardowej, oznacza to, że na taśmach znajdują się kopie zapasowe wcześniej utworzone na danym komputerze. Przenieś (s. 203) te taśmy ręcznie do puli **Wolne taśmy**, jeśli nie potrzebujesz już tych kopii zapasowych.
3. Zdecyduj, czy chcesz tworzyć kopie zapasowe w domyślnej **puli** Acronis (s. 200), czy wolisz utworzyć nową pulę (s. 201).
4. Jeśli wybrana pula nie jest uzupełnialna (s. 383), przenieś do niej wszystkie załadowane taśmy z puli **Wolne taśmy**.
5. Utwórz zarządzany skarbiec centralny (s. 179). Tworząc skarbiec:
 - W polu **Napędy** wybierz całe urządzenie taśmowe. Umożliwi to jednoczesne tworzenie kopii zapasowych komputerów za pomocą różnych napędów, jeśli urządzenie taśmowe jest wyposażone w więcej niż jeden napęd.
 - W polu **Pula taśm** wybierz pulę, w której będą tworzone kopie zapasowe (pulę **Acronis** lub nowo utworzoną pulę).
6. Podczas tworzenia planu tworzenia kopii zapasowych (s. 48):
 - Wybierz utworzony skarbiec jako miejsce docelowe kopii zapasowych.
 - Wybierz schemat tworzenia kopii zapasowych **Dziadek-ojciec-syn (GFS)**.
 - Określ reguły powodujące zachowywanie dziennych kopii zapasowych przez 7 dni, tygodniowych przez 4 tygodnie i miesięcznych bezterminowo.
 - Kliknij **Pokaż typ kopii zapasowej, druga lokalizacja...**, a następnie w polu **Typ kopii zapasowej** wybierz **Pełna/przyrostowa/różnicowa**.
 - W oknie **Zarządzanie taśmami** (s. 124) w ramach opcji tworzenia kopii zapasowych wybierz **Do każdej pełnej kopii zapasowej w obszarze Zawsze używaj wolnej taśmy**.
7. Po utworzeniu pełnej kopii zapasowej możesz wysunąć jej taśmy i wysłać je do innej, bezpiecznej lokalizacji. Jeśli nie masz dostatecznej liczby wolnych taśm, aby kontynuować tworzenie kopii zapasowych, załaduj nowe taśmy i wykonaj kroki 2 i 4.

Rezultat

Kopie zapasowe komputera będą zapisywane na taśmach zgodnie z określonym schematem tworzenia kopii zapasowych. Taśmy z pełnymi kopiami zapasowymi będą wysyłane do innej, bezpiecznej lokalizacji.

6.4 Węzły magazynowania

W kolejnych sekcjach opisano korzystanie z węzłów magazynowania Acronis Backup & Recovery 11 Storage Node.

Węzły magazynowania są dostępne tylko w zaawansowanych wersjach programu Acronis Backup & Recovery 11.

6.4.1 Co to jest węzeł magazynowania?

Węzeł magazynowania Acronis Backup & Recovery 11 Storage Node to serwer przeznaczony do optymalizacji wykorzystania różnych zasobów (takich jak pojemność firmowego magazynu, przepustowości sieci i obciążenia procesorów w komputerach zarządzanych) wymaganych do ochrony danych przedsiębiorstwa. Cel ten jest osiągnięty dzięki organizowaniu lokalizacji służących jako osobne magazyny dla archiwów kopii zapasowych przedsiębiorstwa (skarbcze zarządzane) i zarządzaniu nimi.

Najistotniejszą funkcją węzła magazynowania jest deduplikacja kopii zapasowych przechowywanych w jego skarbcach. Oznacza to, że identyczne dane zostaną uwzględnione w kopii zapasowej tylko raz. Minimalizuje to wykorzystanie sieci podczas tworzenia kopii zapasowej oraz zmniejsza ilość zajmowanego miejsca w archiwum.

Można skonfigurować do 50 węzłów magazynowania.

6.4.2 Obsługiwane typy pamięci masowej

Skarbiec zarządzany można zorganizować:

- na lokalnych dyskach twardych węzła magazynowania,
- w udziale sieciowym,
- w sieci SAN (Storage Area Network),
- w magazynie NAS (Network Attached Storage),
- w bibliotece taśm (s. 191) dołączonej lokalnie do węzła magazynowania.

6.4.3 Operacje wykonywane przez węzły magazynowania

Węzły magazynowania mogą wykonywać następujące operacje na archiwach przechowywanych w skarbcach zarządzanych.

Czyszczenie i sprawdzanie poprawności

Archiwa przechowywane w skarbcach niezarządzanych są obsługiwane przez agenty (s. 376) tworzące te archiwa. Oznacza to, że zadaniem każdego agenta nie jest wyłącznie tworzenie kopii zapasowych danych w archiwum, ale również wykonywanie zadań związanych z obsługą archiwum oraz stosowanie reguł przechowywania i sprawdzania poprawności określonych w planie tworzenia kopii zapasowych (s. 382). Aby zmniejszyć niepotrzebne obciążenie procesora na komputerach zarządzanych, wykonywanie zadań związanych z obsługą można oddelegować do węzła magazynowania. Ponieważ harmonogramy zadań istnieją na komputerze, na którym znajduje się agent — a więc korzysta on z zegara i zdarzeń tego komputera — agent musi zainicjować czyszczenie i sprawdzanie poprawności zgodnie z harmonogramem. Aby było to możliwe, agent musi działać w trybie online. Dalsze czynności są wykonywane w węźle magazynowania.

Tej funkcji nie można wyłączyć w skarbcu zarządzanym. Następne dwie operacje są opcjonalne.

Deduplikacja

Skarbiec zarządzany można skonfigurować jako skarbiec deduplikacji. Oznacza to, że identyczne dane zostaną uwzględnione w kopii zapasowej tylko raz, aby zminimalizować wykorzystanie sieci podczas

tworzenia kopii zapasowej oraz zmniejszyć ilość zajmowanego miejsca w archiwum. Aby uzyskać więcej informacji, zobacz „Deduplikacja” (s. 224).

Szyfrowanie

Skarbiec zarządzany można skonfigurować, tak aby wszystkie zapisywane w nim dane były szyfrowane, a wszystkie odczytywane dane deszyfrowane w sposób przezroczysty przez węzeł magazynowania. Używa się do tego celu klucza szyfrującego skarbca przechowywanego na serwerze węzłów. W przypadku kradzieży nośnika magazynu lub uzyskania do niego dostępu przez osobę nieautoryzowaną odszyfrowanie zawartości skarbca bez dostępu do wspomnianego węzła magazynowania będzie niemożliwe.

Jeśli archiwum jest już zaszyfrowane przez agenta, węzeł magazynowania stosuje własne szyfrowanie po szyfrowaniu wykonanym przez agenta.

6.4.4 Rozpoczęcie pracy z węzłem magazynowania


Wymagania wstępne


Sprawdź, czy:

- serwer zarządzania, konsola i agenty są już zainstalowane.
- Komputer, na którym jest planowana instalacja węzła magazynowania, spełnia wymagania systemowe opisane w dokumentacji instalacji.
- Został pobrany program instalacyjny Acronis Backup & Recovery 11.

Konfigurowanie węzła magazynowania

1. Zainstaluj węzeł magazynowania Acronis Backup & Recovery 11 Storage Node.
 - a. Zaloguj się jako administrator i uruchom program instalacyjny Acronis Backup & Recovery 11.
 - b. Kliknij **Zainstaluj program Acronis Backup & Recovery 11**.
 - c. Zaakceptuj warunki umowy licencyjnej.
 - d. Zaznacz pole wyboru **Przechowywanie kopii zapasowych innych komputerów na tym komputerze**.
 - e. Kliknij **Zarejestruj teraz**, a następnie określ nazwę i hasło użytkownika należącego do grupy Acronis Centralized Admins na komputerze z serwerem zarządzania.

Informacje szczegółowe. Możesz również później dodać węzeł magazynowania, jak opisano w kroku 3.
 - f. Kontynuuj instalację.
2. Utwórz konto dla każdego użytkownika, któremu chcesz zezwolić na dostęp do węzła magazynowania. Pomiń ten krok, jeśli zarówno węzeł magazynowania, jak i komputery użytkowników znajdują się w tej samej domenie Active Directory.
3. Dodaj węzeł magazynowania do serwera zarządzania. Pomiń ten krok, jeśli węzeł magazynowania zarejestrowano w trakcie instalacji.
 - a. Podłącz konsolę do serwera zarządzania i kliknij **Węzły magazynowania** w panelu **Nawigacja**.
 - b. Kliknij  **Dodaj**, a następnie przejdź do czynności opisanych w sekcji „Dodawanie węzła magazynowania do serwera zarządzania” (s. 217).
4. Utwórz zarządzany skarbiec centralny.
 - a. Podłącz konsolę do serwera zarządzania (jeśli nie jest podłączona), a następnie kliknij **Węzły magazynowania** w panelu **Nawigacja**.

- b. Wybierz węzeł magazynowania, a następnie kliknij  **Utwórz skarbiec**. Otworzy się strona **Utwórz skarbiec centralny** ze wstępnie wybranym węzłem magazynowania. Wykonaj pozostałe kroki procedury tworzenia skarbca opisane w sekcji „Tworzenie zarządzanego skarbca centralnego” (s. 179).

Uwaga. Jeśli włączysz deduplikację w skarbcu, pamiętaj, że dodatek Deduplikacja musi być zainstalowany na wszystkich komputerach, których kopie zapasowe są zapisywane w skarbcu. Bez tego dodatku tworzenie kopii zapasowych w skarbcu deduplikacji nie jest możliwe.

Informacje szczegółowe. Określając ścieżki do skarbca i bazy danych deduplikacji, postępuj zgodnie z zaleceniami opisanymi w sekcji „Sprawdzone praktyki dotyczące deduplikacji” (s. 227).

Tworzenie kopii zapasowych w węźle magazynowania

Utwórz lokalny (s. 48) lub scentralizowany (s. 315) plan tworzenia kopii zapasowych. W trakcie tworzenia planu tworzenia kopii zapasowych określ skarbiec zarządzany jako docelowe miejsce przechowywania kopii zapasowych.

Odzyskiwanie z węzła magazynowania

Wykonaj standardowe czynności opisane w sekcji „Tworzenie zadania odzyskiwania” (s. 130).

Zarządzanie węzłami magazynowania

1. Podłącz konsolę do serwera zarządzania.
2. W panelu **Nawigacja** kliknij **Węzły magazynowania**.
3. Wybierz węzeł magazynowania, a następnie wykonaj wymagane operacje opisane w sekcji „Czynności dotyczące węzłów magazynowania” (s. 216).

6.4.5 Uprawnienia użytkownika w węźle magazynowania

Konta użytkowników w węźle magazynowania Acronis Backup & Recovery 11 Storage Node charakteryzują się różnymi uprawnieniami użytkownika.

1. **Acronis Centralized Admins** — administratorzy serwera zarządzania, członkowie grupy Acronis Centralized Admins. Członkowie grupy Acronis Centralized Admins mogą:
 - tworzyć skarbcie centralne przeznaczone do zarządzania przez węzeł magazynowania;
 - dodawać, edytować lub usuwać konta administratorów i użytkowników skarbca;
 - wyświetlać i zarządzać dowolnym archiwum w dowolnym centralnym skarbcu zarządzanym przez węzeł magazynowania;
 - zarządzać indeksowaniem i kompaktowaniem zgodnie z opisem w sekcji „Czynności dotyczące węzłów magazynowania” (s. 216).
2. **Administratorzy skarbca** — grupa lub konta pojedynczych użytkowników w węźle magazynowania wybrane przez administratora serwera zarządzania podczas tworzenia lub edycji skarbca. Administratorzy skarbca mogą wyświetlać wszystkie archiwa w określonym skarbcu zarządzanym i zarządzać nimi. Domyślnie do grupy Administratorzy skarbca jest dodawana grupa Administratorzy w węźle magazynowania.
3. **Użytkownicy skarbca** — grupa lub konta pojedynczych użytkowników w węźle magazynowania wybrane przez administratora serwera zarządzania podczas tworzenia lub edycji skarbca. Użytkownicy skarbca mogą wyświetlać tylko własne archiwa w skarbcu i zarządzać nimi. Domyślnie do użytkowników skarbca jest dodawana grupa Wszyscy w węźle magazynowania.

Zalecenia dotyczące kont użytkowników

Aby zezwolić użytkownikom na dostęp do centralnych skarbców zarządzanych przez węzeł magazynowania, należy dopilnować, aby posiadali oni prawa dostępu do węzła magazynowania za pośrednictwem sieci.

Jeśli komputery użytkowników i komputer z węzłem magazynowania znajdują się w jednej domenie Active Directory, prawdopodobnie nie trzeba wykonywać dalszych kroków: wszyscy użytkownicy są zazwyczaj członkami grupy Użytkownicy domeny i stąd posiadają dostęp do węzła zarządzania.

W przeciwnym razie należy utworzyć konta użytkowników na komputerze z zainstalowanym węzłem magazynowania. Zaleca się utworzenie oddzielnego konta dla każdego użytkownika, który będzie mieć dostęp do węzła magazynowania, tak aby użytkownicy mieli dostęp wyłącznie do własnych archiwów.

Dodatkowe prawa administratorów komputerów

Użytkownik skarbca, który jest na komputerze członkiem grupy Administratorzy, może wyświetlać dowolne archiwa utworzone z *tego komputera* w skarbcu zarządzanym oraz zarządzać nimi — niezależnie od typu swojego konta użytkownika w węźle magazynowania.

Przykład

Załóżmy, że dwóch użytkowników komputera — UserA i UserB — wykonują kopie zapasowe z tego komputera w skarbcu centralnym zarządzanym przez węzeł magazynowania. W węźle magazynowania użytkownicy mają zwykłe (nie administracyjne) konta — odpowiednio UserA_SN i UserB_SN. Podczas tworzenia skarbca zarządzanego oba konta zostały dodane jako użytkownicy skarbca.

Użytkownik UserA ma zwykle dostęp wyłącznie do archiwów utworzonych przez użytkownika UserA (i należących do UserA_SN), natomiast użytkownik UserB ma dostęp wyłącznie do archiwów utworzonych przez użytkownika UserB (i należących do UserB_SN).


Jednak jeśli użytkownik UserA jest członkiem grupy Administratorzy na komputerze, może on dodatkowo korzystać z dostępu do archiwów utworzonych na tym komputerze przez użytkownika UserB — nawet jeśli użytkownik UserA posiada w węźle magazynowania konto zwykłe.





6.4.6 Operacje na węzłach magazynowania

Czynności dotyczące węzłów magazynowania

Aby uzyskać dostęp do czynności

1. Podłącz konsolę do serwera zarządzania.
2. W panelu **Nawigacja** kliknij **Węzły magazynowania**.
3. Czynności wykonuje się przez kliknięcie odpowiednich przycisków na pasku narzędzi.

Zadanie	Czynności
Dodaj węzeł magazynowania do serwera zarządzania	<ol style="list-style-type: none">1. Kliknij  Dodaj.2. W oknie Dodaj węzeł magazynowania (s. 217) określ komputer, na którym jest zainstalowany węzeł magazynowania. <p>Dodanie węzła magazynowania powoduje ustanowienie zaufanej relacji między nim a serwerem zarządzania, tak samo jak w przypadku dodawania komputerów do serwera. Po dodaniu węzła magazynowania do serwera zarządzania będzie można tworzyć w węźle skarbce zarządzane.</p>

Usun węzeł magazynowania z serwera zarządzania	<p>1. Wybierz węzeł magazynowania, który musisz usunąć.</p> <p>2. Kliknij  Usun.</p> <p>Po usunięciu węzła magazynowania z serwera zarządzania skarbce zarządzane przez węzeł znikną z listy skarbców (s. 175) i nie będzie można wykonywać na nich żadnych operacji. Wszystkie plany i zadania wykorzystujące te skarbce zakończą się niepowodzeniem. Wszystkie bazy danych i skarbce na tym węźle magazynowania pozostaną bez zmian.</p> <p>Program umożliwia ponowne dodanie do serwera zarządzania wcześniej usuniętego węzła zarządzania. W wyniku takiej operacji wszystkie skarbce zarządzane przez węzeł magazynowania pojawią się na liście skarbców i staną się ponownie dostępne dla wszystkich planów i zadań, które wcześniej z nich korzystały.</p>
Utwórz centralny skarbiec zarządzany w wybranym węźle magazynowania	<p>1. Wybierz węzeł magazynowania, który będzie zarządzał skarbcem.</p> <p>2. Kliknij  Utwórz skarbiec.</p> <p>Otworzy się strona Utwórz skarbiec centralny (s. 179) ze wstępnie wybranym węzłem magazynowania. Aby utworzyć skarbiec, wykonaj pozostałe kroki procedury.</p>
Wyświetl szczegóły węzła magazynowania	<p>1. Wybierz węzeł magazynowania.</p> <p>2. Kliknij  Wyświetl szczegóły.</p> <p>W oknie Szczegóły węzła magazynowania (s. 218) (którego zawartość jest również dostępna na panelu Informacje w dolnej części widoku Węzły magazynowania) zapoznaj się z informacjami na temat węzła i zarządzanych przez niego skarbców.</p>
Uruchamianie, zatrzymywanie lub przesuwanie kompaktowania na inny termin	<p>W oknie Szczegóły węzła magazynowania (s. 218) kliknij odpowiednie łącze Uruchom kompaktowanie, Zatrzymaj lub Harmonogram kompaktowania.</p>
Uruchamianie lub zatrzymywanie indeksowania	<p>W oknie Szczegóły węzła magazynowania (s. 218) kliknij odpowiednie łącze Uruchom indeksowanie lub Zatrzymaj.</p>
Odśwież listę węzłów magazynowania	<p>Kliknij  Odśwież.</p> <p>Konsola zarządzania zaktualizuje listę węzłów magazynowania o najnowsze informacje z serwera zarządzania. Lista węzłów magazynowania odświeża się automatycznie na podstawie zdarzeń. Mimo to, ze względu na pewne opóźnienie dane z serwera zarządzania mogą nie pojawić się natychmiast. Po ręcznym odświeżeniu wyświetlane są najbardziej aktualne dane.</p>

Dodawanie węzła magazynowania do serwera zarządzania

Aby dodać węzeł magazynowania

1. W polu **Adres IP/nazwa** wprowadź nazwę komputera, na którym znajduje się węzeł magazynowania, lub jego adres IP albo kliknij **Przeglądaj** i wyszukaj komputer w sieci.
 Jako nazwy węzła magazynowania użyj w pełni kwalifikowanej nazwy domeny (FQDN), to znaczy w pełni określonej nazwy domeny kończącej się domeną najwyższego poziomu. Nie należy wprowadzać ustawień „127.0.0.1” lub „localhost” jako adresu IP lub nazwy węzła magazynowania. Ustawienia te nie są prawidłowe nawet w przypadku, gdy serwer zarządzania i węzeł magazynowania znajdują się na tym samym komputerze, ponieważ po wdrożeniu

scentralizowanego planu tworzenia kopii zapasowych wykorzystującego węzeł magazynowania każdy agent będzie próbował uzyskać dostęp do węzła, tak jakby był on zainstalowany na hoście agenta.

2. Aby podać prawidłowe konto użytkownika komputera, kliknij **Opcje>>** i określ następujące parametry:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena). Konto użytkownika musi być członkiem grupy administratorów komputera.
- **Hasło.** Hasło konta.

Zaznacz pole wyboru **Zapisz hasło**, aby zapamiętać hasło konta.

3. Kliknij **OK**.

Rejestracja wymaga udziału węzła magazynowania, zatem nie może nastąpić, kiedy komputer jest w trybie offline.

Szczegóły węzła magazynowania

Na czterech kartach okna **Szczegóły węzła magazynowania** znajdują się wszystkie informacje dotyczące wybranego węzła Acronis Backup & Recovery 11 Storage Node. Informacje te są także dostępne na panelu **Informacje**.

Właściwości węzła magazynowania

Na tej karcie są wyświetlane następujące informacje dotyczące wybranego węzła magazynowania:

- **Nazwa** — nazwa komputera z zainstalowanym węzłem magazynowania
- **Adres IP hosta** — adres IP komputera z zainstalowanym węzłem magazynowania
- **Dostępność:**
 - **Nieznany** — ten status jest wyświetlany po dodaniu węzła magazynowania lub uruchomieniu usługi serwera zarządzania, a przed pierwszym połączeniem serwera z węzłem.
 - **Online** — węzeł magazynowania jest dostępny dla serwera zarządzania. Oznacza to, że ostatnie połączenie serwera zarządzania z węzłem zostało nawiązane pomyślnie. Próby połączeń są wykonywane co dwie minuty.
 - **Offline** — węzeł magazynowania jest niedostępny.
 - **Wycofany** — węzeł magazynowania został zarejestrowany na innym serwerze zarządzania. Oznacza to, że nie jest możliwe sterowanie węzłem z bieżącego serwera zarządzania.
- **Archiwa** — całkowita liczba archiwów przechowywanych we wszystkich skarbcach zarządzanych przez węzeł zarządzania.
- **Kopie zapasowe** — całkowita liczba kopii zapasowych przechowywanych w archiwach we wszystkich skarbcach zarządzanych przez węzeł magazynowania.
- **Indeksowanie** — działanie indeksowania powoduje deduplikację danych zapisanych podczas tworzenia kopii zapasowej w skarbcu deduplikacji. Indeksowanie jest uruchamiane po wykonaniu każdej kopii zapasowej. Aby dowiedzieć się więcej na temat indeksowania, zobacz „Zasada działania deduplikacji” (s. 225).
 - **Bezczynne** — indeksowanie nie jest uruchomione. Indeksowanie można uruchomić, klikając łącze **Uruchom indeksowanie**.
 - **Uruchomione** — indeksowanie jest uruchomione. Indeksowanie można zatrzymać, klikając łącze **Zatrzymaj**. Indeksowanie jest operacją wymagającą zaangażowania dużej ilości zasobów, więc czasem warto je zatrzymać w celu przydzielenia dodatkowych zasobów innym


procesom, które są w danym momencie ważniejsze. Zatrzymanie indeksowania jest zalecane wyłącznie w przypadku absolutnej konieczności. Należy je następnie ponownie uruchomić w najbliższym sprzyjającym momencie. Im dłuższe opóźnienie indeksowania, tym więcej danych w skarbcu nie zostanie zdeduplikowanych i tym większe będzie wykorzystanie miejsca na dysku.

- **Kompaktowanie** — zadanie kompaktowania usuwa z magazynu danych deduplikacji nieużywane bloki danych. Aby dowiedzieć się więcej na temat kompaktowania, zobacz „Zasada działania deduplikacji” (s. 225).
 - **Bezczynne** — kompaktowanie nie jest uruchomione. Kompaktowanie można uruchomić, klikając łącze **Uruchom kompaktowanie**.
 - **Uruchomione** — kompaktowanie jest uruchomione. Kompaktowanie można zatrzymać, klikając łącze **Zatrzymaj**.
- **Harmonogram kompaktowania** — parametry harmonogramu zadania kompaktowania. Kliknij łącze **Harmonogram kompaktowania**, aby zmienić harmonogram zadania kompaktowania. Program umożliwia skonfigurowanie tylko zdarzeń czasowych (Codziennie (s. 76), Co tydzień (s. 78) oraz Co miesiąc (s. 80)). Ustawienie wstępne: Rozpocznij zadanie co **1 tydzień w niedzielę o 3:00:00**.

Statystyka

Ta karta zawiera informacje na temat rozmiarów danych oryginalnych i po utworzeniu kopii zapasowej we wszystkich skarbcach zarządzanych wybranego węzła magazynowania.

Skarbce

Na tej karcie znajduje się lista skarbców zarządzanych przez wybrany węzeł magazynowania. Kliknij  **Odśwież**, aby zaktualizować listę skarbców o najnowsze informacje z serwera zarządzania.

Indeksowanie

Ta karta umożliwia sprawdzenie bieżącego statusu indeksowania skarbców deduplikacji węzła magazynowania oraz przeglądanie daty i godziny ostatniego uruchomienia tej operacji.

Konfiguracja węzła magazynowania przy użyciu szablonu administracyjnego Acronis Administrative Template

Poniżej podano parametry węzła magazynowania Acronis Backup & Recovery 11 Storage Node, które można skonfigurować przy użyciu szablonu administracyjnego Acronis Administrative Template. Aby uzyskać informacje na temat sposobu stosowania szablonu administracyjnego, zobacz Jak załadować szablon Acronis Administrative Template (s. 360).

Parametry związane z kompaktowaniem

Ponieważ kopie zapasowe są usuwane ze skarbca deduplikacji, magazyn danych deduplikacji (s. 225) może zawierać nieużywane bloki danych, do których nie ma już odwołań w żadnej kopii zapasowej. Węzeł magazynowania przetwarza magazyn danych w celu usunięcia tych nieużywanych elementów. Ta operacja jest nazywana kompaktowaniem. Kompaktowanie jest wykonywane przez zadanie kompaktowania.

Za każdym razem, kiedy uruchamiane jest zadanie kompaktowania, węzeł magazynowania decyduje, czy wykonać kompaktowanie. W tym celu węzeł kompaktowania:

1. Sprawdza rozmiar danych z kopii zapasowych usuniętych ze skarbca od czasu ostatniego kompaktowania.

2. Na podstawie parametru **Compacting Trigger Rough Estimation Threshold** ustala, czy rozmiar ten jest znaczący w porównaniu z pozostałymi danymi w kopii zapasowej.
3. Jeśli tak, na podstawie parametru **Compacting Trigger Threshold** ustala, czy magazyn danych deduplikacji zawiera istotną liczbę nieużywanych elementów. Jeśli tak, węzeł magazynowania przeprowadza kompaktowanie.

Poniżej przedstawiono parametry.

Compacting Trigger Rough Estimation Threshold

Opis: określa względny rozmiar danych w kopii zapasowej pozostających w skarbku deduplikacji, poniżej którego przeprowadza się sprawdzanie nieużywanych elementów (zobacz parametr **Compacting Trigger Threshold**).

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **90**

Parametr **Compacting Trigger Rough Estimation Threshold** umożliwia pominięcie sprawdzania nieużywanych elementów (a tym samym pominięcie kompaktowania) w przypadku, gdy zawartość skarbca nie uległa znacznej zmianie.

Im wyższa wartość parametru, tym częściej będzie wykonywane sprawdzanie nieużywanych elementów. Wartość **100** oznacza, że sprawdzanie będzie wykonywane przy każdym uruchomieniu zadania kompaktowania.

Sposób działania. Załóżmy, że wartość parametru wynosi **90**, a w skarbku znajduje się 100 GB danych w kopiach zapasowych. Nie jest istotne, czy dane te są zduplikowane. Po usunięciu kilku kopii zapasowych rozmiar danych w kopiach wynosi 80 GB. W takim przypadku:

- a. Rozmiar usuniętych danych wynosi 20 GB, a rozmiar danych pozostałych wynosi 80 GB. Stosunek usuniętych danych do pozostałych wynosi więc $20 \text{ GB} / 80 \text{ GB} = 0,25$ lub 25 procent.
- b. Węzeł magazynowania oblicza względny rozmiar pozostałych danych w następujący sposób: $100 \text{ procent} - 25 \text{ procent} = 75 \text{ procent}$.
- c. Ponieważ względny rozmiar jest mniejszy niż **90** procent, węzeł magazynowania rozpoczyna wyszukiwanie nieużywanych elementów.

Compacting Trigger Threshold

Opis: Określa w procentach ilość elementów użytych w magazynie danych deduplikacji, poniżej której następuje kompaktowanie.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **90**

Ponieważ kompaktowanie wymaga użycia dużej ilości zasobów, powinno się odbywać dopiero po zgromadzeniu odpowiednio dużej ilości nieużywanych elementów.

Parametr **Compacting Trigger Threshold** umożliwia ustawienie zależności pomiędzy dodatkowym miejscem wymaganym do przechowywania nieużywanych elementów a częstotliwością kompaktowania. Im większa wartość tego parametru, tym mniej nieużywanych elementów będzie się znajdowało w magazynie danych, ale kompaktowanie będzie się odbywało częściej.

Sprawdzenie jest wykonywane dopiero po sprawdzeniu odsetka pozostałych w skarbku danych kopii zapasowych (zobacz **Compacting Trigger Rough Estimation Threshold**).

Inne parametry

Log Cleanup Rules

Określa sposób czyszczenia dziennika węzła magazynowania.

Ten parametr ma następujące ustawienia:

Max Size

Opis: Określa maksymalny (w kilobajtach) rozmiar folderu z dziennikiem węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **1048576** (1 GB)

Percentage To Keep

Opis: Określa procentowo maksymalny rozmiar dziennika, który ma być zachowany podczas czyszczenia.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **95**

Client Connection Limit

Opis: Określa maksymalną liczbę równoczesnych połączeń z węzłem magazynowania ze strony agentów tworzących kopie zapasowe, odzyskujących dane lub wykonujących operacje na archiwach (takie jak sprawdzanie poprawności, replikacja lub czyszczenie).

Możliwe wartości: Dowolna liczba całkowita z zakresu od **1** do **2147483647**

Wartość domyślna: **10**

Agenty programu Acronis Backup & Recovery 11 łączą się z węzłem magazynowania w celu uzyskania dostępu do jego skarbów zarządzanych podczas tworzenia kopii zapasowych, odzyskiwania lub w celu wykonania operacji na archiwum. Parametr **Client Connection Limit** określa maksymalną liczbę połączeń, jaką może równocześnie obsłużyć węzeł magazynowania.

Po osiągnięciu tego ograniczenia wobec agentów oczekujących na połączenie węzeł magazynowania zastosuje kolejkę kopii zapasowych (zobacz następny parametr).

Zobacz również parametr **Fast Operation Connection Limit**.

Backup Queue Limit

Opis: Określa maksymalną liczbę agentów w kolejce kopii zapasowych węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **1** do **2147483647**

Wartość domyślna: **50**

Kolejka kopii zapasowych to lista agentów oczekujących na połączenie z węzłem magazynowania w celu utworzenia kopii zapasowej, odzyskania danych lub wykonania operacji na archiwum (zobacz poprzedni parametr). Lista ta obejmuje również agenty aktualnie połączone z węzłem magazynowania w powyższych celach.

Jeśli agent próbuje ustanowić takie połączenie w chwili, gdy liczba agentów w kolejce kopii zapasowych jest równa wartości parametru **Backup Queue Limit**, węzeł magazynowania nie umieści agenta w kolejce.

W takim przypadku połączenie agenta z węzłem magazynowania nie powiedzie się. Odpowiednie zadanie zostanie zatrzymane ze statusem **Błąd**.

Zobacz również parametr **Fast Operation Queue Limit**.

Fast Operation Connection Limit

Opis: Określa maksymalną liczbę jednoczesnych połączeń z węzłem magazynowania w celach innych niż tworzenie kopii zapasowych, odzyskiwanie danych i operacje na archiwach.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **1** do **2147483647**

Wartość domyślna: **10**

Komponenty programu Acronis Backup & Recovery 11 mogą łączyć się z węzłem magazynowania w celu wyświetlenia zawartości skarbca lub wykonania innych szybkich operacji. Parametr **Fast**

Operation Connection Limit określa maksymalną liczbę połączeń, jaką może równocześnie obsłużyć węzeł magazynowania.

Po osiągnięciu tego ograniczenia wobec komponentów oczekujących na połączenie węzeł magazynowania zastosuje kolejkę szybkich operacji (zobacz następny parametr).

Zobacz również parametr **Client Connection Limit**.

Fast Operation Queue Limit

Opis: Określa maksymalną liczbę komponentów programu Acronis Backup & Recovery 11 w kolejce szybkich operacji (zobacz poprzedni parametr).

Możliwe wartości: Dowolna liczba całkowita z zakresu od 1 do **2147483647**

Wartość domyślna: **50**

Kolejka szybkich operacji to lista komponentów oczekujących na połączenie w celu wykonania szybkich operacji, takich jak wyświetlenie zawartości skarbca.

Jeśli liczba komponentów w kolejce jest równa wartości parametru **Fast Operation Queue Limit**, węzeł magazynowania nie umieści w kolejce kolejnego komponentu próbującego nawiązać połączenie. W takim przypadku odpowiednia operacja zakończy się niepowodzeniem.

Zobacz również parametr **Backup Queue Limit**.

Vault Metadata Databases Path

Opis: Określa ścieżkę do folderu, w którym są przechowywane bazy danych skarbca, zwane również bazami danych metadanych.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość

domyślna:

%AllUsersProfile%\Acronis\BackupAndRecovery\ASN\VaultMetadataDatabases

Baza danych skarbca zawiera informacje o archiwach i kopiach zapasowych przechowywanych w skarbcu. Podczas tworzenia lub dołączania skarbca węzeł magazynowania umieszcza jego bazę danych w folderze określonym przez ten parametr.

Zmiana tego parametru nie wpływa na już istniejące bazy danych skarbców. Jeśli chcesz przenieść te bazy danych do nowego folderu, odłącz (s. 178) odpowiednie skarbcy, a następnie dołącz (s. 184) je do tego samego węzła magazynowania.

Check Hash Value On Server Side

Opis: Określa, czy sprawdzać wartości skrótów bloków danych wysyłanych do skarbca deduplikacji

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

Podczas wysyłania bloku danych do skarbca deduplikacji agent wysyła także odcisk bloku, zwany również wartością skrótu.

Parametr **Check Hash Value On Server Side** określa, czy węzeł magazynowania musi sprawdzać zgodność wartości skrótu z blokiem danych. Takie sprawdzenie dodatkowo obciąża węzeł magazynowania.

W normalnych warunkach nie jest ono konieczne. Wartość tego ustawienia można zmienić na **True**, aby dodatkowo zabezpieczyć proces deduplikacji.

Jeśli blok danych nie jest zgodny z jego wartością skrótu, operacja tworzenia kopii zapasowej nie powiedzie się.

Vault Warnings and Limits

Określa ilość wolnego miejsca w skarbku (zarówno bezwzględnie, jak i procentowo), poniżej której w dzienniku rejestrowane jest ostrzeżenie lub błąd.

Ten parametr ma następujące ustawienia:

Vault Free Space Warning Limit

Opis: Określa ilość wolnego miejsca w skarbku zarządzanym (w megabajtach), poniżej której rejestrowane jest ostrzeżenie w dzienniku węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **200**

Wolne miejsce w skarbku to ilość wolnego miejsca na nośniku, takim jak wolumin dysku, na którym znajduje się skarbiec.

Jeśli ilość wolnego miejsca w skarbku jest równa lub mniejsza od wartości ustawienia **Vault Free Space Warning Limit**, w dzienniku węzła magazynowania rejestrowane jest ostrzeżenie wskazujące ten skarbiec. Ostrzeżenia węzła magazynowania można wyświetlić na pulpicie nawigacyjnym.

Vault Free Space Warning Percentage

Opis: Określa ilość wolnego miejsca w skarbku zarządzanym (wyrażoną jako procent jego całkowitego rozmiaru), poniżej której rejestrowane jest ostrzeżenie w dzienniku węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **10**

Całkowity rozmiar skarbca to suma wolnego miejsca w skarbku oraz rozmiaru wszystkich archiwów znajdujących się w tym skarbku.

Na przykład przyjmijmy, że na woluminie dysku znajdują się dwa skarbcie: skarbiec A i skarbiec B. Przyjmijmy ponadto, że rozmiar archiwów w skarbku A wynosi 20 GB, a rozmiar archiwów w skarbku B — 45 GB.

Jeśli na woluminie jest 5 GB wolnego miejsca, całkowity rozmiar skarbca A wynosi $20\text{ GB} + 5\text{ GB} = 25\text{ GB}$, a skarbca B — $45\text{ GB} + 5\text{ GB} = 50\text{ GB}$, niezależnie od rozmiaru woluminu.

Procent wolnego miejsca w skarbku to iloraz ilości wolnego miejsca w skarbku i całkowitego rozmiaru skarbca. W poprzednim przykładzie w skarbku A jest $5\text{ GB} / 25\text{ GB} = 20\%$ wolnego miejsca, a w skarbku B — $5\text{ GB} / 50\text{ GB} = 10\%$ wolnego miejsca.

Jeśli procent wolnego miejsca w skarbku jest równy lub mniejszy od wartości ustawienia **Vault Free Space Warning Percentage**, w dzienniku węzła magazynowania rejestrowane jest ostrzeżenie wskazujące ten skarbiec. Ostrzeżenia węzła magazynowania można wyświetlić na pulpicie nawigacyjnym.

Uwaga: Parametry **Vault Free Space Warning Limit** i **Vault Free Space Warning Percentage** są od siebie niezależne: po osiągnięciu któregośkolwiek z tych progów zostanie zarejestrowane ostrzeżenie.

Vault Free Space Error Limit

Opis: Określa ilość wolnego miejsca w skarbku zarządzanym (w megabajtach), poniżej której rejestrowany jest błąd w dzienniku węzła magazynowania, a skarbiec zamykany jest dla wszelkich kopii zapasowych.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **50**

Jeśli ilość wolnego miejsca w skarbku jest równa lub mniejsza od wartości ustawienia **Vault Free Space Error Limit**, w dzienniku węzła magazynowania rejestrowany jest błąd. Tworzenie kopii zapasowych w skarbku będzie kończyć się niepowodzeniem aż do momentu, gdy ilość wolnego miejsca znajdzie się powyżej limitu.

Vault Database Free Space Warning Limit

Opis: Określa ilość wolnego miejsca (w megabajtach) na woluminie zawierającym bazę danych skarbca zarządzanego, poniżej której rejestrowane jest ostrzeżenie w dzienniku węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **20**

Jeśli ilość wolnego miejsca na woluminie zawierającym bazę danych skarbca zarządzanego jest mniejsza niż wartość ustawienia **Vault Database Free Space Warning Limit**, w dzienniku węzła magazynowania rejestrowane jest ostrzeżenie wskazujące ten skarbiec. Ostrzeżenia węzła magazynowania można wyświetlić na pulpicie nawigacyjnym.

Baza danych jest przechowywana w węźle magazynowania w folderze lokalnym, którego nazwa została określona w parametrze **Vault Metadata Database Path**.

Vault Database FreeSpace Error Limit

Opis: Określa ilość wolnego miejsca (w megabajtach) na woluminie zawierającym bazę danych skarbca zarządzanego, poniżej której rejestrowany jest błąd w dzienniku węzła magazynowania, a skarbiec zamykany jest dla wszelkich kopii zapasowych.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **10**

Jeśli ilość wolnego miejsca na dysku zawierającym bazę danych skarbca zarządzanego jest mniejsza niż wartość ustawienia **Vault Database Free Space Error Limit**, w dzienniku węzła magazynowania rejestrowany jest błąd. Tworzenie kopii zapasowych w skarbku będzie kończyć się niepowodzeniem aż do momentu, gdy ilość wolnego miejsca znajdzie się powyżej limitu.

Błędy węzła magazynowania można wyświetlić na pulpicie nawigacyjnym.

Baza danych jest przechowywana w węźle magazynowania w folderze lokalnym, którego nazwa została określona w parametrze **Vault Metadata Database Path**.

6.4.7 Deduplikacja

W tej sekcji omówiono deduplikację, czyli mechanizm mający na celu eliminację powtarzających się danych przez zachowywanie w archiwach tylko jednego egzemplarza identycznych elementów.

Omówienie

Deduplikacja to proces minimalizowania miejsca zajmowanego przez dane, który polega na wykrywaniu powtarzających się danych i zachowywaniu tylko jednego egzemplarza identycznych elementów.

Deduplikacja umożliwia również zmniejszenie obciążenia sieci: jeśli podczas tworzenia kopii zapasowej program wykryje dane będące duplikatami już przechowywanych danych, jego zawartość nie będzie przesyłana przez sieć.

Program Acronis Backup & Recovery 11 zdeduplikuje kopie zapasowe zapisane w skarbku zarządzanym, jeśli włączysz deduplikację podczas tworzenia skarbca. Skarbiec z włączoną deduplikacją nazywa się **skarbcem deduplikacji**. Dodatek deduplikacji agenta musi być zainstalowany

na każdym komputerze, na którym tworzona jest kopia zapasowa w takim skarbku. Wykonywanie kopii zapasowej w takim skarbku bez użycia tego dodatku jest niemożliwe.

Deduplikacja przeprowadzana jest na blokach danych. Rozmiar bloku wynosi **4 KB w przypadku kopii zapasowych na poziomie dysku i od 1 B do 256 KB w przypadku kopii zapasowych na poziomie plików**. Każdy plik o rozmiarze mniejszym niż 256 KB jest uznawany za blok danych. Pliki większe niż 256 KB są dzielone na bloki o rozmiarze 256 KB.

Program Acronis Backup & Recovery 11 przeprowadza deduplikację w dwóch krokach:

Deduplikacja w źródle

Jest to deduplikacja wykonywana na komputerze zarządzanym podczas tworzenia kopii zapasowej. Agent wykorzystuje węzeł magazynowania do ustalenia, jakie dane poddać deduplikacji i nie przesyła bloków danych, których duplikaty już znajdują się w skarbku.

Deduplikacja w miejscu docelowym

Wykonywana w skarbku po ukończeniu tworzenia kopii zapasowej. Węzeł magazynowania analizuje zawartość skarbca i deduplikuje zawarte w nim dane.

Podczas tworzenia planu tworzenia kopii zapasowych można wyłączyć w tym planie funkcję deduplikacji w miejscu źródłowym. Może to prowadzić do szybszego tworzenia kopii zapasowych, ale jednocześnie — do większego obciążenia sieci i węzła magazynowania.

Baza danych deduplikacji

Węzeł magazynowania Acronis Backup & Recovery 11 Storage Node zarządzający skarbkiem deduplikacji utrzymuje bazę danych deduplikacji, która zawiera wartości skrótów wszystkich bloków danych przechowywanych w skarbku z wyjątkiem tych, które nie mogą być poddane deduplikacji, na przykład plików zaszyfrowanych.

Baza danych deduplikacji jest przechowywana w lokalnym folderze węzła magazynowania. Podczas tworzenia skarbca można określić ścieżkę do bazy danych.

Rozmiar bazy danych deduplikacji wynosi około 1,5 procent całkowitego rozmiaru unikatowych danych przechowywanych w skarbku. Innymi słowy, każdy terabajt nowych danych (niebędących duplikatami) dodaje około 15 GB do bazy danych.

W przypadku uszkodzenia bazy danych lub utracenia węzła magazynowania zawartość skarbca pozostaje nienaruszona, ale nowy węzeł magazynowania ponownie skanuje skarbiec, najpierw odtwarzając bazę danych skarbca, a następnie bazę danych deduplikacji.

Zasada działania deduplikacji

Deduplikacja w źródle

Podczas tworzenia kopii zapasowej w skarbku deduplikacji, komponent Acronis Backup & Recovery 11 Agent oblicza wartość odcisku każdego bloku danych. Taki odcisk jest często zwany *wartością skrótu*.

Przed przesłaniem bloku danych do skarbca agent wysyła zapytanie do bazy danych deduplikacji, aby ustalić, czy wartość skrótu bloku jest taka sama jak jednego z bloków już przechowywanych. Jeśli tak, agent wysyła tylko wartość skrótu. W przeciwnym razie wysyła sam blok. Węzeł magazynowania zapisuje otrzymane bloki danych w pliku tymczasowym.

Niektórych danych, jak np. zaszyfrowanych plików lub bloków dysków o niestandardowym rozmiarze, nie można deduplikować. Agent zawsze wysyła takie dane do skarbca bez obliczania wartości skrótu.

Aby uzyskać więcej informacji na temat ograniczeń deduplikacji, zobacz Ograniczenia deduplikacji (s. 229).

Po ukończeniu procesu tworzenia kopii zapasowej skarbiec zawiera powstałą kopię zapasową oraz plik tymczasowy z unikatowymi blokami danych. Plik tymczasowy zostanie przetworzony na następnym etapie. Plik kopii zapasowej (plik TIB) zawiera wartości skrótów i dane, których nie można deduplikować. Dalsze przetwarzanie tej kopii zapasowej nie jest konieczne. Możesz łatwo odzyskać z niej dane.

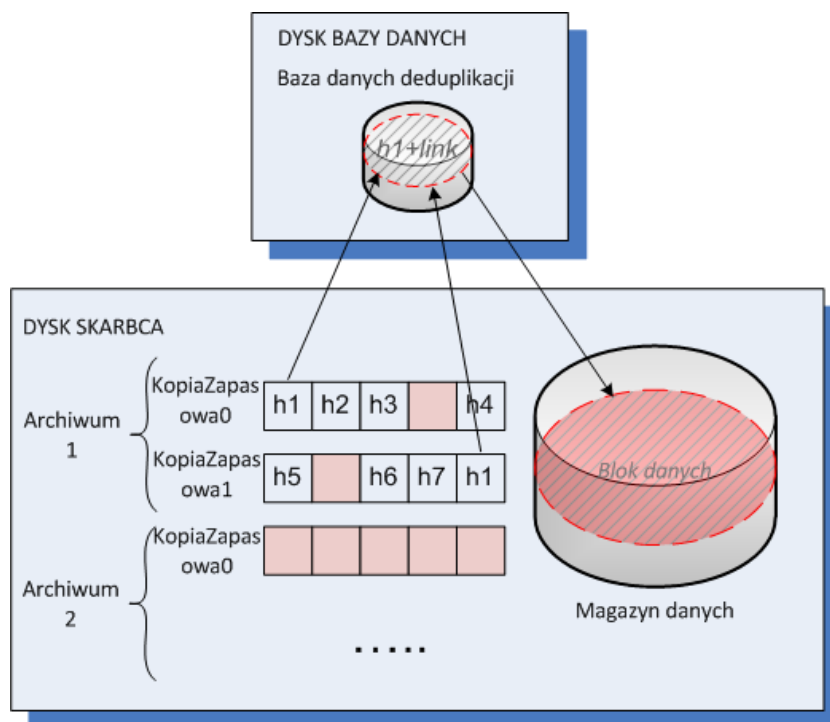
Deduplikacja w miejscu docelowym

Gdy zakończy się tworzenie kopii zapasowej w skarbcu deduplikacji, węzeł magazynowania uruchomi **czynność indeksowania**. Czynność ta powoduje deduplikację danych w skarbcu w następującej kolejności:

1. Przenosi bloki danych z pliku tymczasowego do specjalnego pliku wewnątrz skarbca, gdzie zapisuje zduplikowane elementy tylko raz. Plik ten nazywany jest **magazynem danych deduplikacji**.
2. Zapisuje w bazie danych deduplikacji wartości skrótów i łączy niezbędne do „złożenia” danych po deduplikacji.
3. Po przeniesieniu wszystkich bloków danych usuwa plik tymczasowy.

W rezultacie magazyn danych zawiera pewną liczbę unikatowych bloków danych. Każdy blok ma jedno lub kilka odwołań z kopii bezpieczeństwa. Odwołania są zawarte w bazie danych deduplikacji. Kopie bezpieczeństwa pozostają nienaruszone. Zawierają wartości skrótów oraz dane, których nie można deduplikować.

Poniższy diagram ilustruje rezultat deduplikacji w miejscu docelowym.



Wykonanie czynności indeksowania może zająć sporo czasu. Stan tego działania można sprawdzić na serwerze zarządzania, wybierając odpowiedni węzeł magazynowania i klikając **Wyświetl szczegóły** (s. 218). W tym oknie można także uruchomić lub zatrzymać to działanie.

Kompaktowanie

Gdy ze skarbca zostanie usunięta — ręcznie lub podczas czyszczenia — jedna lub więcej kopii zapasowych bądź archiwów, magazyn danych może zawierać bloki, do których nie odwołuje się żadne archiwum. Elementy takie są usuwane przez **zadanie kompaktowania**, które jest zaplanowanym zadaniem wykonywanym przez węzeł magazynowania.

Domyślnie zadanie kompaktowania jest uruchamiane w każdą niedzielę o godzinie 03:00. Można zmienić jego harmonogram, wybierając odpowiedni węzeł magazynowania, klikając **Wyświetl szczegóły** (s. 218), a następnie **Harmonogram kompaktowania**. Na karcie tej można również ręcznie uruchomić lub zatrzymać to zadanie.

Ponieważ usuwanie nieużywanych bloków wymaga użycia dużej ilości zasobów, zadanie kompaktowania usuwa je tylko po zgromadzeniu wystarczającej ilości danych do usunięcia. Próg jest określony przez parametr konfiguracyjny **Próg uruchomienia kompaktowania** (s. 219).

Najefektywniejsza deduplikacja

Poniżej wymieniono sytuacje, w których deduplikacja przynosi najlepszy efekt:

- Tworzenie kopii zapasowej podobnych danych z różnych źródeł w **trybie pełnej kopii zapasowej**. Sytuacja taka ma miejsce, gdy tworzona jest kopia zapasowa systemów operacyjnych i aplikacji wdrożonych w sieci z jednego źródła.
- Tworzenie **przyrostowych kopii zapasowych** podobnych danych z różnych źródeł, pod warunkiem, że **zmiany danych są również podobne**. Sytuacja taka ma miejsce, gdy wdrażane są aktualizacje systemów, a następnie tworzona jest przyrostowa kopia zapasowa.
- Tworzenie **przyrostowych kopii zapasowych** danych, które same się nie zmieniają, ale **zmienia się ich lokalizacja**. Sytuacja taka ma miejsce, gdy wiele fragmentów danych krąży w sieci lub w jednym systemie. Każdy ruch fragmentu danych jest uwzględniany w przyrostowej kopii zapasowej, co powoduje, że kopia się rozrasta, a nie zawiera żadnych nowych danych. Deduplikacja ułatwia rozwiązanie tego problemu: za każdym razem, gdy określony element pojawi się w nowym miejscu, zapisywane jest odwołanie do tego elementu, a nie on sam.

Deduplikacja i przyrostowe kopie zapasowe

W przypadku losowych zmian danych deduplikacja przyrostowej kopii zapasowej nie przyniesie większych efektów, ponieważ:

- Elementy zdeduplikowane, które nie uległy zmianie, nie są uwzględniane w przyrostowej kopii zapasowej.
- Elementy zdeduplikowane, które uległy zmianie, nie są już identyczne i dlatego nie będą dłużej deduplikowane.

Deduplikacja i kopie zapasowe bazy danych

Deduplikacja nie jest zbyt wydajnym rozwiązaniem przy regularnym tworzeniu kopii zapasowych bazy danych. Jest to związane z faktem, że zmiany w bazie danych są zazwyczaj unikatowe i dlatego nie można ich deduplikować. Zalecamy tworzenie kopii zapasowych baz danych w skarbcu bez aktywnej funkcji deduplikacji.

Sprawdzone praktyki dotyczące deduplikacji

Deduplikacja to złożony proces zależny od wielu czynników.

Najważniejsze czynniki mające wpływ na szybkość deduplikacji to:

- Szybkość dostępu do bazy danych deduplikacji

- Rozmiar pamięci RAM węzła magazynowania
- Liczba skarbów deduplikacji utworzonych w węźle magazynowania.

Aby zwiększyć wydajność deduplikacji, zastosuj poniższe zalecenia.

Umieść bazę danych deduplikacji i skarb deduplikacji na osobnych urządzeniach fizycznych

Aby zwiększyć szybkość dostępu do bazy danych deduplikacji, baza i skarb muszą znajdować się na osobnych urządzeniach fizycznych.

Najlepszą praktyką jest przydzielenie skarbowi i bazie danych specjalnych urządzeń. Jeśli nie jest to możliwe, unikaj przynajmniej umieszczania skarba lub bazy danych na wspólnym dysku z systemem operacyjnym. Jest to związane z dużą liczbą operacji odczytu/zapisu twardego dysku wykonywanych przez system operacyjny, co znacząco zwalnia deduplikację.

Wybór dysku bazy danych deduplikacji

- Baza danych musi znajdować się na dysku niewymiennym. Nie należy umieszczać bazy danych deduplikacji na zewnętrznych dyskach wymiennych.
- Ważne jest zapewnienie minimalnego czasu dostępu do dysku. Zaleca się używanie szybkiego dysku IDE (min. 7200 obr./min), dysku SCSI, lub dysku Solid-State Drive (SSD) klasy Enterprise.
- Wolumin z bazą danych deduplikacji powinien dysponować przynajmniej 10 GB wolnego miejsca. W przypadku tworzenia kopii zapasowych dużej liczby komputerów wymagana wielkość wolnego miejsca może przekroczyć 10 GB.
- Rozmiar miejsca na dysku wymaganego do poprawnego działania bazy danych deduplikacji można oszacować za pomocą następującego równania:

$$S = U / 64 + 10$$

gdzie

S — rozmiar dysku (w GB)

U — planowany rozmiar unikatowych danych w magazynie danych deduplikacji (w GB).

Jeśli na przykład planowany rozmiar unikatowych danych w magazynie danych deduplikacji wynosi U=5 TB, baza danych deduplikacji będzie wymagała wolnego miejsca na dysku o rozmiarze co najmniej

$$S = 5 \cdot 1024 / 64 + 10 = 90 \text{ GB}$$

Wybór dysku skarba deduplikacji

W celu zapobiegania utracie danych zaleca się użycie macierzy RAID 10, 5 lub 6. Macierz RAID 0 nie jest zalecana, ponieważ nie jest odporna na awarie. Macierz RAID 1 nie jest zalecana z powodu względnie niewielkiej prędkości. Do tego zastosowania nadają się zarówno dyski lokalne, jak i SAN.

8 GB pamięci RAM na 1 TB unikatowych danych

To jest zalecenie przy założeniu najbardziej pesymistycznego scenariusza. Nie trzeba go ściśle przestrzegać, jeśli nie występują problemy z wydajnością deduplikacji. Jeśli jednak deduplikacja przebiega zbyt wolno, sprawdź parametr **Zajęte miejsce** skarba deduplikacji. Dodanie większej ilości pamięci RAM w węźle magazynowania może znacząco podnieść prędkość deduplikacji.

Ogólna zasada mówi, że większy rozmiar pamięci RAM umożliwia większy rozmiar bazy danych deduplikacji przy założeniu takiej samej szybkości deduplikacji.

Tylko jeden skarbiec deduplikacji na każdy węzeł magazynowania

Zdecydowanie zaleca się utworzenie w węźle magazynowania tylko jednego skarbcia deduplikacji. W innym przypadku cała dostępna pamięć RAM zostanie proporcjonalnie rozdzielona między poszczególne skarbcie.

64-bitowy system operacyjny

W celu zapewnienia optymalnej wydajności deduplikacji zaleca się instalację węzła magazynowania w 64-bitowym systemie operacyjnym. Na komputerze nie powinny być uruchomione aplikacje o dużym zapotrzebowaniu na zasoby systemowe, takie jak systemy zarządzania bazami danych (DBMS) lub systemy planowania zasobów (ERP).

Procesor wielordzeniowy z zegarem co najmniej 2,5 GHz

Zaleca się użycie procesora o co najmniej 4 rdzeniach i częstotliwości zegara nie niższej niż 2,5 GHz.

Wystarczająca ilość wolnego miejsca w skarbcu

Indeksowanie kopii zapasowej wymaga tyle wolnego miejsca, ile zajmują dane kopii bezpośrednio po jej zapisaniu w skarbcu. Bez kompresji lub deduplikacji w miejscu źródłowym wartość ta jest równa rozmiarowi oryginalnych danych uwzględnionych w danej operacji tworzenia kopii zapasowej.

Szybka sieć LAN

Zaleca się użycie sieci LAN 1-Gbit. Pozwoli ona na równoległe wykonywanie 5-6 kopii zapasowych z deduplikacją bez wyraźnej redukcji szybkości.

Tworzenie kopii zapasowej typowego komputera przed utworzeniem kopii zapasowych kilku komputerów o podobnej zawartości

W przypadku tworzenia kopii zapasowych kilku komputerów o podobnej zawartości zaleca się najpierw utworzenie kopii zapasowej jednego komputera, a następnie odczekanie do zakończenia indeksowania danych uwzględnionych w kopii zapasowej. Po tym czasie tworzenie kopii zapasowych pozostałych komputerów będzie szybsze dzięki wydajnej deduplikacji. Z uwagi na zaindeksowanie kopii zapasowej pierwszego komputera większość danych znajduje się już w magazynie danych deduplikacji.

Tworzenie kopii zapasowych poszczególnych komputerów o różnych porach

Jeśli stworzysz kopie zapasowe dużej liczby komputerów, rozłóż w czasie operacje tworzenia kopii zapasowych. W tym celu utwórz kilka planów tworzenia kopii zapasowych z różnymi harmonogramami.

Konfigurowanie powiadomień o alertach

Zaleca się skonfigurowanie powiadomienia o alercie (s. 357) „Skarbce” w opcjach serwera zarządzania. Ułatwi to szybką reakcję na niecodzienne sytuacje. Szybka reakcja na alert „Istnieje skarbiec z małą ilością wolnego miejsca” może na przykład zapobiec wystąpieniu błędu podczas późniejszej operacji tworzenia kopii zapasowej w skarbcu.

Ograniczenia deduplikacji

Typowe ograniczenia

Deduplikacji nie można wykonać w archiwum chronionym hasłem. Bloki danych archiwów chronionych hasłem są przechowywane w kopiach zapasowych tak, jakby znajdowały się w skarbcu bez aktywnej funkcji deduplikacji.

Jeśli chcesz chronić archiwum, jednocześnie zezwalając na jego deduplikację, nie szyfruj hasłem archiwum, ale sam skarbiec deduplikacji. Można to uczynić podczas tworzenia skarbca.

Tworzenie kopii zapasowych na poziomie dysku

Deduplikacji bloków dysku nie można dokonać, jeśli rozmiar jednostki alokacji woluminu — zwanej także rozmiarem klastra lub rozmiarem bloku — jest niepodzielny przez 4 KB.

Wskazówka: Rozmiar jednostki alokacji na większości woluminów NTFS i ext3 wynosi 4 KB. Umożliwia to deduplikację na poziomie bloków. Inne przykładowe rozmiary jednostki alokacji umożliwiające deduplikację na poziomie bloków to 8 KB, 16 KB oraz 64 KB.

Kopia zapasowa na poziomie plików

Deduplikacja pliku nie dojdzie do skutku, jeśli jest on zaszyfrowany, a pole wyboru **Pliki zaszyfrowane zapisz w archiwach w postaci odszyfrowanej** nie jest zaznaczone w opcjach tworzenia kopii zapasowych (domyślnie pole to nie jest zaznaczone).

Deduplikacja i strumienie danych NTFS

W systemie plików NTFS z plikiem można skojarzyć jeden lub więcej zestawów danych, zwanych często *alternatywnymi strumieniami danych*.

Alternatywne strumienie danych takiego pliku są wraz z nim także umieszczane w kopii zapasowej. Jednak strumienie takie nigdy nie podlegają deduplikacji, nawet w przypadku deduplikacji samego pliku.

7 Operacje na archiwach i kopiach zapasowych

7.1 Sprawdzanie poprawności archiwów i kopii zapasowych

Operacja sprawdzania poprawności polega na sprawdzeniu, 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 lub woluminu polega na obliczeniu sumy kontrolnej każdego bloku danych zapisanego w kopii zapasowej. Obie procedury intensywnie wykorzystują zasoby komputera.

Sprawdzenie poprawności archiwum oznacza sprawdzenie kopii zapasowych w tym archiwum. Sprawdzanie poprawności skarbca (lub lokalizacji) oznacza sprawdzanie wszystkich archiwów przechowywanych w tym skarbcu (lokalizacji).

Udana operacja sprawdzania poprawności oznacza wysokie prawdopodobieństwo pomyślnego odzyskania danych. Jednak w jej trakcie nie są sprawdzane wszystkie czynniki, które mają wpływ na proces odzyskiwania. Po utworzeniu kopii zapasowej systemu operacyjnego gwarancję pomyślnego odzyskania danych można uzyskać jedynie na podstawie testu, który polega na odzyskaniu danych w środowisku startowym na zapasowy dysk twardy. Upewnij się przynajmniej, że poprawność kopii zapasowej można z powodzeniem sprawdzić przy użyciu nośnika startowego.

Różne metody tworzenia zadania sprawdzania poprawności

Zadanie sprawdzania poprawności można najprościej utworzyć za pomocą strony **Sprawdzanie poprawności**. Na stronie tej można od razu sprawdzić poprawność lub ustalić harmonogram sprawdzania poprawności dowolnej kopii zapasowej, archiwum lub skarbca, które są dostępne w ramach posiadanych uprawnień.

Sprawdzanie poprawności archiwum lub najnowszej kopii zapasowej w archiwum można zaplanować w ramach planu tworzenia kopii zapasowych. Aby uzyskać więcej informacji, zobacz Tworzenie planu tworzenia kopii zapasowych (s. 48).

Aby uzyskać dostęp do strony **Sprawdzanie poprawności**, najpierw wybierz obiekt, którego poprawność chcesz sprawdzić: skarbiec, archiwum lub kopię zapasową.

- Aby wybrać skarbiec, w panelu **Nawigacja** kliknij ikonę **Skarbce** i wybierz skarbiec, rozwijając drzewo skarbców w widoku **Skarbce** lub bezpośrednio w panelu **Nawigacja**.
- Aby wybrać archiwum, wybierz skarbiec, a następnie w widoku **Skarbiec** zaznacz kartę **Widok archiwum** i kliknij nazwę archiwum.
- Aby wybrać kopię zapasową, w **Widoku archiwum** wybierz archiwum, rozwiń je, klikając przycisk rozwijania po lewej stronie obok nazwy archiwum, a następnie kliknij kopię zapasową.

Po wybraniu obiektu przeznaczonego do sprawdzenia poprawności z menu kontekstowego wybierz **Sprawdź poprawność**. Zostanie otwarta strona **Sprawdzanie poprawności** ze wstępnie wybranym obiektem jako źródłem. Wystarczy wybrać czas sprawdzania poprawności oraz (opcjonalnie) podać nazwę zadania.

Aby utworzyć zadanie sprawdzania poprawności, wykonaj poniższe kroki

Elementy do sprawdzenia poprawności

Sprawdź poprawność

Wybierz obiekt do sprawdzenia poprawności:

Archiwum (s. 238) — w tym przypadku należy określić samo archiwum.

Kopia zapasowa (s. 233) — najpierw określ archiwum. Następnie wybierz żadaną kopię zapasową zawartą w tym archiwum.

Skarbiec (s. 233) — wybierz skarbiec (lub inną lokalizację), który zawiera archiwa do sprawdzenia poprawności.

Poświadczenia (s. 233)

[Opcjonalnie] Jeśli konto zadania nie ma wystarczających uprawnień dostępu do źródła, podaj poświadczenia dostępu.

Czas sprawdzania poprawności

Uruchom sprawdzanie poprawności (s. 234)

Określ czas i częstotliwość sprawdzania poprawności.

Parametry zadania

Nazwa zadania

[Opcjonalnie] Wprowadź unikatową nazwę zadania sprawdzania poprawności. Dobrze dobrana nazwa umożliwi szybką identyfikację zadania spośród innych zadań.

Poświadczenia zadania (s. 234)

[Opcjonalnie] Zadanie sprawdzania poprawności będzie uruchamiane w imieniu użytkownika, który je utworzył. W razie potrzeby można zmienić poświadczenia zadania.

Komentarze

[Opcjonalnie] Wprowadź komentarze do zadania.

Po skonfigurowaniu wszystkich wymaganych ustawień kliknij **OK**, aby utworzyć zadanie sprawdzania poprawności.

7.1.1 Wybór archiwum

Wybieranie archiwum

1. Wprowadź pełną ścieżkę do lokalizacji archiwum w polu **Ścieżka** lub wybierz wymaganą lokalizację w drzewie (s. 132).

W przypadku pracy na komputerze uruchamianym z nośnika startowego:

- Aby uzyskać dostęp do skarbca zarządzanego, w polu **Ścieżka** wpisz następujący ciąg:
bsp://adres_węzła/nazwa_skarbca/
- Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.

2. Wybierz archiwum w tabeli po prawej stronie drzewa. Tabela przedstawia nazwy archiwów znajdujących się w każdej wybranej przez użytkownika lokalizacji.

Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

3. Kliknij **OK**.

7.1.2 Wybór kopii zapasowej

Aby określić kopię zapasową w celu sprawdzenia poprawności

1. W górnym panelu wybierz kopię zapasową według daty/godziny jej utworzenia.
W dolnej części okna program wyświetli zawartość wybranej kopii zapasowej, co ułatwia znalezienie właściwej kopii.
2. Kliknij **OK**.

7.1.3 Wybór skarbca

Aby wybrać skarbiec lub lokalizację

1. Wprowadź pełną ścieżkę do skarbca (lokalizacji) w polu **Ścieżka** lub wybierz żądaną lokalizację w drzewie.
 - Aby wybrać skarbiec centralny, rozwiń grupę **Centralne** i kliknij odpowiedni skarbiec.
 - Aby wybrać skarbiec osobisty, rozwiń grupę **Osobiste** i kliknij odpowiedni skarbiec.
 - Aby wybrać folder lokalny (płytę CD/DVD lub podłączone lokalnie urządzenie taśmowe), rozwiń grupę **Foldery lokalne** i kliknij wymagany folder.
 - Aby wybrać udział sieciowy, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.
 - Aby wybrać folder przechowywany w udziale NFS, rozwiń grupę **Dyski NFS** i kliknij folder.
 - Aby wybrać serwer **FTP** lub **SFTP**, rozwiń odpowiednią grupę i kliknij folder na serwerze.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejść przy użyciu programu do przechwytywania pakietów.

Aby ułatwić wybranie właściwego skarbca, tabela przedstawia nazwy archiwów znajdujących się w każdym wybranym skarbcu. Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

1. Kliknij **OK**.

7.1.4 Poświadczenia dostępu do źródła

Określ poświadczenia wymagane do uzyskania dostępu do lokalizacji, w której znajduje się archiwum kopii zapasowej.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
 - **Użyj poświadczeń zadania**
Program uzyska dostęp do lokalizacji za pomocą poświadczeń konta zadania określonego w sekcji **Parametry zadania**.
 - **Użyj następujących poświadczeń**
Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Użyj tej opcji, jeśli konto zadania nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.
Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejść przy użyciu programu do przechwytywania pakietów.

7.1.5 Czas sprawdzania poprawności

Ponieważ operacja sprawdzania poprawności wymaga użycia dużej ilości zasobów, najlepiej zaplanować jej wykonanie wtedy, gdy obciążenie zarządzanego komputera jest najmniejsze. Jednak, aby dowiedzieć się jak najszybciej, czy dane nie są uszkodzone i czy można je pomyślnie odzyskać, należy rozpocząć sprawdzanie poprawności natychmiast po utworzeniu zadania.

Wybierz jedną z następujących opcji:

- **Teraz** — aby rozpocząć zadanie sprawdzania poprawności natychmiast po jego utworzeniu, to znaczy po kliknięciu OK na stronie Sprawdzanie poprawności.
- **Później** — aby rozpocząć zadanie sprawdzania poprawności w określonym dniu i o określonej godzinie.
Określ odpowiednie parametry:
 - **Data i godzina** — data i godzina rozpoczęcia zadania.
 - **Zadanie zostanie uruchomione ręcznie (nie planuj zadania)** — zaznacz to pole wyboru, jeśli chcesz uruchomić zadanie ręcznie w późniejszym terminie.
- **Według harmonogramu** — aby zaplanować uruchomienie zadania. Więcej informacji na temat konfigurowania parametrów harmonogramu można znaleźć w sekcji Planowanie (s. 74).

7.1.6 Poświadczenia zadania

Określ poświadczenia konta, na którym zadanie będzie uruchamiane.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń bieżącego użytkownika**
Zadanie będzie uruchamiane przy użyciu poświadczeń, z którymi zalogował się użytkownik rozpoczynający zadania. Jeśli zadanie ma zostać uruchomione według harmonogramu, w momencie zakończenia tworzenia zadania użytkownik zostanie poproszony o aktualne hasło użytkownika.
- **Użyj następujących poświadczeń**
Zadanie będzie zawsze uruchamiane przy użyciu poświadczeń określonych przez użytkownika, niezależnie od tego, czy zadanie będzie uruchamiane ręcznie, czy wykonywane według harmonogramu.
Określ:
 - **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).

- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Więcej informacji na temat używania poświadczeń w programie Acronis Backup & Recovery 11 można znaleźć w sekcji Właściciele i poświadczenia (s. 32).

Aby dowiedzieć się więcej na temat operacji dostępnych w zależności od uprawnień użytkownika, zobacz sekcję Uprawnienia użytkownika na komputerze zarządzanym.

7.2 Eksportowanie archiwów i kopii zapasowych

Operacja eksportu tworzy kopię archiwum lub samowystarczalną częściową kopię archiwum w lokalizacji określonej przez użytkownika. Oryginalne archiwum pozostaje nietknięte.

Operację eksportu można zastosować do następujących obiektów:

- **Jednego archiwum** — zostanie utworzona dokładna kopia archiwum.
- **Jednej kopii zapasowej** — zostanie utworzone archiwum składające się z jednej pełnej kopii zapasowej. Eksport przyrostowej lub różnicowej kopii zapasowej odbywa się przez konsolidację poprzednich kopii zapasowych z najbliższą pełną kopią zapasową.
- **Wybranych kopii zapasowych** należących do tego samego archiwum — archiwum wynikowe będzie zawierać tylko określone kopie zapasowe. Konsolidacja jest wykonywana zgodnie z wymaganiami użytkownika, więc archiwum wynikowe może zawierać pełne, przyrostowe lub różnicowe kopie zapasowe.
- **Cały skarbiec**, który można wyeksportować za pomocą interfejsu wiersza polecenia. Aby uzyskać więcej informacji, zobacz Opis wiersza polecenia programu Acronis Backup & Recovery 11.

Scenariusze użycia

Eksport umożliwia wyodrębnienie określonej kopii zapasowej z łańcucha przyrostowych kopii zapasowych w celu szybkiego jej odzyskania, zapisania na nośniku wymiennym bądź odłączanym albo w innym celu.

Przykład. W przypadku tworzenia kopii zapasowej danych do lokalizacji zdalnej przez niestabilne połączenie sieciowe lub połączenie o niskiej przepustowości (np. podczas tworzenia kopii zapasowej przez sieć WAN przy użyciu sieci VPN), zaleca się zapisać początkową pełną kopię zapasową na nośnik odłączany. Następnie można przesłać nośnik do lokalizacji zdalnej. Tam kopia zapasowa zostanie wyeksportowana z nośnika na dysk docelowy. Kolejne przyrostowe kopie zapasowe, które zazwyczaj są znacznie mniejsze, będą mogły być przenoszone przez sieć.

W wyniku eksportu skarbca zarządzanego na nośnik odłączany otrzymuje się przenośny skarbiec niezarządzany, którego można użyć w ramach następujących scenariuszy:

- przechowywanie kopii skarbca lub najważniejszych archiwów w innej lokalizacji,
- fizyczny przewóz skarbca do oddległego oddziału firmy,
- odzyskanie danych bez dostępu do węzła magazynowania w przypadku problemów komunikacji sieciowej lub awarii węzła magazynowania,
- odzyskanie samego węzła magazynowania.

Eksport ze skarbca znajdującego się na dysku twardym na urządzenie taśmowe może być uważany za proste etapowe tworzenie archiwum na żądanie.

Nazwa archiwum wynikowego

Domyślnie wyeksportowane archiwum dziedziczy nazwę oryginalnego archiwum. Ponieważ przechowywanie wielu archiwów o takich samych nazwach w tej samej lokalizacji nie jest wskazane, następujące czynności stosowane do domyślnej nazwy archiwum są niedostępne:

- eksportowanie części archiwum do tej samej lokalizacji
- eksportowanie archiwum lub jego części do lokalizacji, w której istnieje archiwum o tej samej nazwie
- eksportowanie archiwum lub jego części dwukrotnie do tej samej lokalizacji

W każdym z powyższych przypadków należy podać nazwę archiwum unikatową w folderze lub skarbcu docelowym. Jeśli trzeba ponownie wykonać zadanie eksportu przy użyciu tej samej nazwy archiwum, należy najpierw usunąć archiwum powstałe w wyniku poprzedniej operacji eksportu.

Opcje archiwum wynikowego

Domyślnie wyeksportowane archiwum dziedziczy opcje oryginalnego archiwum, w tym szyfrowanie i hasło. W przypadku eksportowania archiwum chronionego hasłem pojawi się monit o podanie hasła. Jeżeli oryginalne archiwum jest zaszyfrowane, zostanie zastosowane hasło w celu zaszyfrowania archiwum wynikowego.

Lokalizacje źródłowe i docelowe

Kiedy konsola jest podłączona do **komputera zarządzanego**, można wyeksportować archiwum lub jego część do i z dowolnej lokalizacji dostępnej dla agenta znajdującego się na komputerze. Dotyczy to skarbców osobistych, lokalnie podłączonych urządzeń taśmowych i nośników wymiennych, a w zaawansowanych wersjach produktu — zarządzanych i niezarządzanych skarbców centralnych.

Kiedy konsola jest podłączona do **serwera zarządzania**, dostępne są dwie metody eksportu:

- Eksport ze **skarbcza zarządzanego**. Zadanie eksportu jest wykonywane przez węzeł magazynowania, który zarządza skarbciem. Miejscem docelowym może być udział sieciowy lub folder lokalny węzła magazynowania.
- Eksport z **niezarządzanego skarbcza centralnego**. Zadanie eksportu jest wykonywane przez agenta zainstalowanego na komputerze zarządzanym określonym przez użytkownika. Miejscem docelowym może być dowolna lokalizacja, do której agent ma dostęp, w tym skarbiec zarządzany.

Wskazówka. Podczas konfigurowania zadania eksportu danych do zarządzanego skarbcza deduplikacji wybierz komputer, na którym zainstalowany jest dodatek deduplikacji do agenta. W przeciwnym razie zadanie eksportu zakończy się niepowodzeniem.

Operacja na zadaniach eksportu

Zadanie eksportu jest uruchamiane natychmiast po zakończeniu jego konfiguracji. Zadanie eksportu można zatrzymać lub usunąć tak samo jak każde inne zadanie.

Ukończone zadanie eksportu można uruchomić ponownie w dowolnej chwili. Przedtem należy usunąć archiwum utworzone w wyniku uruchomienia poprzedniego zadania, jeśli to archiwum nadal istnieje w skarbciu docelowym. W przeciwnym razie zadanie zakończy się niepowodzeniem. Nie można edytować zadania eksportu w celu określenia innej nazwy archiwum docelowego (to jest ograniczenie).

Wskazówka. Można zastosować scenariusz etapowy ręcznie, regularnie wykonując zadanie usuwania archiwum, a po nim zadanie eksportu.

Różne metody tworzenia zadania eksportu

Zadanie eksportu można najprościej utworzyć za pomocą strony **Eksport**. Ta strona umożliwia wyeksportowanie dowolnej kopii zapasowej lub dowolnego archiwum, które są dostępne dla użytkownika.

Dostęp do strony **Eksport** można uzyskać z widoku **Skarbcze**. Kliknij prawym przyciskiem myszy obiekt do wyeksportowania (archiwum lub kopia zapasowa) i wybierz **Eksport** z menu kontekstowego.

Aby uzyskać dostęp do strony **Eksport**, najpierw wybierz obiekt do sprawdzania poprawności — archiwum lub kopię zapasową.

1. Wybierz skarbiec. W tym celu w panelu **Nawigacja** kliknij ikonę **Skarbcze** i wybierz skarbiec, rozwijając drzewo skarbów w widoku **Skarbcze** lub bezpośrednio w panelu **Nawigacja**.
2. Aby wybrać archiwum, wybierz skarbiec, a następnie w widoku **Skarbiec** zaznacz kartę **Widok archiwum** i kliknij nazwę archiwum.
3. Aby wybrać kopię zapasową, w **Widoku archiwum** wybierz archiwum, rozwiń je, klikając przycisk rozwijania po lewej stronie obok nazwy archiwum, a następnie kliknij kopię zapasową.

Po wybraniu obiektu przeznaczonego do sprawdzenia poprawności z menu kontekstowego wybierz **Eksportuj**. Zostanie otwarta strona **Eksport** ze wstępnie wybranym obiektem jako źródłem. Wystarczy tylko wybrać miejsce docelowe i (opcjonalnie) podać nazwę zadania.

Aby wyeksportować archiwum lub kopię zapasową, wykonaj poniższe czynności.

Elementy do wyeksportowania

Eksportuj

Wybierz typ obiektów do wyeksportowania:

Archiwum — w tym przypadku należy określić samo archiwum.

Kopie zapasowe — należy najpierw określić archiwum, a następnie wybrać żądane kopie zapasowe zawarte w tym archiwum.

Przeglądaj

Wybierz **Archiwum** (s. 238) lub **Kopie zapasowe** (s. 238).

Pokaż poświadczenia dostępu (s. 238)

[Opcjonalnie] Jeśli konto zadania nie ma wystarczających uprawnień dostępu do źródła, podaj poświadczenia dostępu.

Lokalizacja eksportu

Przeglądaj (s. 239)

Określ ścieżkę do lokalizacji, w której zostanie utworzone nowe archiwum.

Należy podać charakterystyczną nazwę i komentarz do nowego archiwum.

Pokaż poświadczenia dostępu (s. 240)

[Opcjonalnie] Jeśli poświadczenia zadania nie są wystarczające, podaj poświadczenia dostępu do lokalizacji docelowej.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby uruchomić zadanie eksportu.

W jego wyniku program wyświetli **Stan wykonania** zadania w widoku **Plany i zadania tworzenia kopii zapasowych**. Po zakończeniu zadania w oknie **Informacje o zadaniu** pojawi się ostateczny stan wykonania zadania.

7.2.1 Wybór archiwum

Wybieranie archiwum

1. Wprowadź pełną ścieżkę do lokalizacji archiwum w polu **Ścieżka** lub wybierz wymaganą lokalizację w drzewie (s. 132).

W przypadku serwera zarządzania w drzewie folderów wybierz skarbiec zarządzany.

2. Wybierz archiwum w tabeli po prawej stronie drzewa. Tabela przedstawia nazwy archiwów znajdujących się w każdej wybranej przez użytkownika lokalizacji.

Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

3. Kliknij **OK**.

7.2.2 Wybór kopii zapasowej

Aby określić kopie zapasowe do wyeksportowania

1. U góry okna zaznacz odpowiednie pola wyboru.

Aby się upewnić, że została wybrana właściwa kopia zapasowa, kliknij kopię i spójrz na dolną tabelę, w której są wyświetlane woluminy znajdujące się w wybranej kopii zapasowej.

Aby uzyskać informacje na temat woluminu, kliknij go prawym przyciskiem myszy, a następnie wybierz **Informacja**.

2. Kliknij **OK**.

7.2.3 Poświadczenia dostępu do źródła

Określ poświadczenia wymagane w celu uzyskania dostępu do lokalizacji, w której znajduje się archiwum źródłowe lub kopia zapasowa.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń bieżącego użytkownika**

Program uzyska dostęp do lokalizacji przy użyciu poświadczeń bieżącego użytkownika.

- **Użyj następujących poświadczeń**

Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Użyj tej opcji, jeśli konto zadania nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.

Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejść przy użyciu programu do przechwytywania pakietów.

7.2.4 Wybór miejsca docelowego

Określ miejsce docelowe przechowywania wyeksportowanego obiektu. Eksportowanie kopii zapasowych do tego samego archiwum jest niedozwolone.

1. Wybór miejsca docelowego eksportu

Wprowadź pełną ścieżkę do miejsca docelowego w polu **Ścieżka** lub wybierz żądane miejsce docelowe w drzewie.

- Aby wyeksportować dane do niezarządzanego skarbca centralnego, rozwiń grupę **Skarbce centralne** i kliknij skarbiec.
- Aby wyeksportować dane do skarbca osobistego, rozwiń grupę **Skarbce osobiste** i kliknij skarbiec.
- Aby wyeksportować dane do folderu lokalnego na komputerze, rozwiń grupę **Foldery lokalne** i kliknij żądany folder.
- Aby wyeksportować dane do udziału sieciowego, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

Uwaga dla użytkowników systemu Linux: Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.

- Aby wyeksportować dane na serwer **FTP** lub **SFTP**, wpisz nazwę i adres serwera w polu **Ścieżka** w następujący sposób:

ftp://serwer_ftp:numer_portu lub **sftp://serwer_sftp:numer_portu**

Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.

Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder na serwerze.

Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję **Użyj dostępu anonimowego**.

Zgodnie z oryginalną specyfikacją protokołu FTP poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako zwykły tekst. Oznacza to, że nazwę użytkownika i hasło można przechwycić przy użyciu programu do przechwytywania pakietów.

- Aby wyeksportować dane na lokalnie podłączone urządzenie taśmowe, rozwiń grupę **Napędy taśmowe**, a następnie kliknij żądane urządzenie. W autonomicznych wersjach programu Acronis Backup & Recovery 11 urządzenia taśmowe są dostępne tylko w przypadku aktualizacji z wersji Acronis Backup & Recovery 10. Aby uzyskać więcej informacji na temat używania taśm, zobacz sekcję „Urządzenia taśmowe” (s. 191).

W przypadku serwera zarządzania drzewo folderów zawiera:

- grupę **Foldery lokalne** dla potrzeb eksportu danych na lokalne dyski twarde węzła magazynowania;
- grupę **Foldery sieciowe** dla potrzeb eksportu danych do udziału sieciowego. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

Uwaga dla użytkowników systemu Linux: Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.

2. Korzystanie z tabeli archiwów

Aby łatwiej było wybrać właściwe miejsce docelowe, w tabeli po prawej stronie są wyświetlane nazwy archiwów znajdujących się w poszczególnych lokalizacjach wybranych w drzewie.

Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

3. Nadawanie nazwy nowemu archiwum

Domyślnie wyeksportowane archiwum dziedziczy nazwę oryginalnego archiwum. Ponieważ przechowywanie wielu archiwów o takich samych nazwach w tej samej lokalizacji nie jest wskazane, następujące czynności stosowane do domyślnej nazwy archiwum są niedostępne:

- eksportowanie części archiwum do tej samej lokalizacji
- eksportowanie archiwum lub jego części do lokalizacji, w której istnieje archiwum o tej samej nazwie
- eksportowanie archiwum lub jego części dwukrotnie do tej samej lokalizacji

W każdym z powyższych przypadków należy podać nazwę archiwum unikatową w folderze lub skarbcu docelowym. Jeśli trzeba ponownie wykonać zadanie eksportu przy użyciu tej samej nazwy archiwum, należy najpierw usunąć archiwum powstałe w wyniku poprzedniej operacji eksportu.

7.2.5 Poświadczenia dostępu do miejsca docelowego

Określ poświadczenia wymagane w celu uzyskania dostępu do lokalizacji archiwum wynikowego. Właścicielem archiwum będzie użytkownik mający określoną nazwę.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń bieżącego użytkownika**
Program uzyska dostęp do lokalizacji docelowej przy użyciu poświadczeń bieżącego użytkownika.
- **Użyj następujących poświadczeń**
Program uzyska dostęp do miejsca docelowego przy użyciu określonych poświadczeń. Użyj tej opcji, jeśli konto zadania nie ma uprawnień dostępu do miejsca docelowego.
Określ:
 - **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
 - **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejść przy użyciu programu do przechwytywania pakietów.

7.3 Montowanie obrazu

Zamontowanie woluminów z kopii zapasowej (obrazu) dysku umożliwia dostęp do woluminów tak, jakby były one dyskami fizycznymi. Podczas jednej operacji montowania można zamontować kilka woluminów zawartych w jednej kopii zapasowej. Operacja montowania jest dostępna, gdy konsola jest połączona z zarządzanym komputerem, na którym działa system Windows lub Linux.

Zamontowanie woluminów w trybie do odczytu/zapisu umożliwia modyfikowanie zawartości kopii zapasowej, czyli zapisywanie, przenoszenie, tworzenie, usuwanie plików lub folderów i uruchamianie programów składających się z jednego pliku.

Woluminy można montować, jeśli kopia zapasowa dysku jest przechowywana w folderze lokalnym (z wyjątkiem nośników wymiennych), strefie Acronis Secure Zone lub udziale sieciowym.

Scenariusze użycia

- **Udostępnianie:** zamontowane obrazy można łatwo udostępniać użytkownikom w sieci.
- **Rozwiązanie odzyskiwania z wykorzystaniem rezerwowej bazy danych:** zamontuj obraz zawierający bazę danych SQL z niedawno uszkodzonego komputera. Umożliwi to dostęp do bazy danych do czasu odzyskania uszkodzonego komputera.
- **Czyszczenie z wirusów w trybie offline:** jeśli komputer został zaatakowany, administrator wyłącza go, uruchamia za pomocą nośnika startowego i tworzy obraz. Następnie administrator montuje obraz w trybie odczytu/zapisu, skanuje go i czyści za pomocą programu antywirusowego, a na końcu odzyskuje komputer.
- **Sprawdzanie błędów:** jeśli odzyskiwanie nie powiodło się z powodu błędu dysku, zamontuj obraz w trybie odczytu/zapisu. Następnie sprawdź, czy na zamontowanym dysku nie ma błędów za pomocą polecenia **chkdsk /r**.

Aby zamontować obraz, wykonaj poniższe czynności.

Źródło

Archiwum (s. 242)

Określ ścieżkę do lokalizacji archiwum i wybierz archiwum zawierające kopie zapasowe dysków.

Kopia zapasowa (s. 243)

Wybierz kopię zapasową.

Poświadczenia dostępu (s. 243)

[Opcjonalnie] Podaj poświadczenia dla lokalizacji archiwum.

Ustawienia montowania

Woluminy (s. 243)

Wybierz woluminy, które chcesz zamontować, i skonfiguruj ustawienia montowania każdego woluminu: przypisz literę lub wprowadź punkt montowania, wybierz tryb dostępu do odczytu i zapisu lub tylko do odczytu.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby zamontować woluminy.

7.3.1 Wybór archiwum

Wybieranie archiwum

1. Wprowadź pełną ścieżkę do lokalizacji w polu **Ścieżka** lub wybierz odpowiedni folder w drzewie folderów.

- Jeśli archiwum znajduje się w magazynie Acronis Online Backup Storage, kliknij **Zaloguj** i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę **Magazyn kopii zapasowych online** i wybierz konto.

W przypadku kopii zapasowych zapisanych w magazynie Acronis Online Backup Storage nie są obsługiwane operacje eksportowania i montowania.

- Jeśli archiwum znajduje się w skarbcu centralnym, rozwiń grupę **Centralne** i kliknij skarbiec.
- Jeśli archiwum znajduje się w skarbcu osobistym, rozwiń grupę **Osobiste** i kliknij skarbiec.
- Jeśli archiwum znajduje się w folderze lokalnym na komputerze, rozwiń grupę **Foldery lokalne** i kliknij odpowiedni folder.

Jeśli archiwum znajduje się na nośniku wymiennym, na przykład na płycie DVD, najpierw włóż ostatnią płytę DVD, a następnie zgodnie z wyświetlanymi monitami wkładaj kolejno pozostałe płyty, zaczynając od pierwszej.

- Jeśli archiwum znajduje się w udziale sieciowym, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

Uwaga dla użytkowników systemu Linux: Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.

- Jeśli archiwum znajduje się na serwerze **FTP** lub **SFTP**, w polu **Ścieżka** wpisz nazwę lub adres serwera w następujący sposób:

ftp://serwer_ftp:numer_portu lub **sftp://serwer_sftp:numer_portu**

Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.

Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder.

Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję **Użyj dostępu anonimowego**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przechwycić przy użyciu programu do przechwytywania pakietów.

- Jeśli archiwum znajduje się na podłączonym lokalnie urządzeniu taśmowym, rozwiń grupę **Napędy taśmowe** i kliknij odpowiednie urządzenie.

W przypadku pracy na komputerze uruchamianym z nośnika startowego:

- Aby uzyskać dostęp do skarbca zarządzanego, w polu **Ścieżka** wpisz następujący ciąg:
bsp://adres_węzła/nazwa_skarbca/
- Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.

2. Wybierz archiwum w tabeli po prawej stronie drzewa. Tabela przedstawia nazwy archiwów znajdujących się w każdym wybranym przez użytkownika skarbca lub folderze.

Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

3. Kliknij **OK**.

7.3.2 Wybór kopii zapasowej

Aby wybrać kopię zapasową:

1. Wybierz jedną z kopii zapasowych według daty/godziny jej utworzenia.
2. Aby ułatwić wybranie właściwej kopii zapasowej, w tabeli poniżej przedstawione są woluminy znajdujące się w wybranej kopii zapasowej.

Aby uzyskać informacje na temat woluminu, kliknij go prawym przyciskiem myszy, a następnie kliknij **Informacja**.

3. Kliknij **OK**.

7.3.3 Poświadczenia dostępu

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń bieżącego użytkownika**

Program uzyska dostęp do lokalizacji przy użyciu poświadczeń bieżącego użytkownika.

- **Użyj następujących poświadczeń**

Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Tej opcji należy użyć, gdy konto bieżącego użytkownika nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.

Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejść przy użyciu programu do przechwytywania pakietów.

7.3.4 Wybór woluminu

Wybierz woluminy, które chcesz zamontować i skonfiguruj parametry montowania każdego z wybranych woluminów w następujący sposób:

1. Zaznacz pole wyboru obok wszystkich woluminów, które chcesz zamontować.
2. Kliknij wybrany wolumin, aby ustawić jego parametry montowania.
 - **Tryb dostępu** — wybierz tryb dostępu, w którym chcesz zamontować wolumin:
 - **Tylko do odczytu** — umożliwia przeglądanie i otwieranie plików w kopii zapasowej bez dokonywania żadnych zmian.
 - **Odczyt/zapis** — w tym trybie program może modyfikować zawartość kopii zapasowej i tworzy w tym celu przyrostową kopię zapasową, w której zapisuje zmiany.


- **Przypisz literę** (w systemie Windows) — Program Acronis Backup & Recovery 11 przypisze nieużywaną literę do montowanego woluminu. W razie konieczności można wybrać inną literę z listy rozwijanej.
 - **Punkt zamontowania** (w systemie Linux) — określ katalog, w którym chcesz zamontować wolumin.
3. Jeśli do zamontowania wybrano kilka woluminów, kliknij każdy z nich, aby ustawić jego parametry montowania, co zostało opisane w poprzednim kroku.
 4. Kliknij **OK**.

7.3.5 Zarządzanie zamontowanymi obrazami

Po zamontowaniu woluminu można przy użyciu menedżera plików przeglądać pliki i foldery zawarte w kopii zapasowej i kopiować wybrane pliki w dowolne miejsce. Dlatego w razie potrzeby skopiowania tylko kilku plików i folderów z kopii zapasowej woluminu nie ma konieczności przeprowadzania całej procedury odzyskiwania.


Przeglądanie zawartości obrazów


Przeglądanie zawartości zamontowanych woluminów umożliwia wyświetlanie i modyfikowanie zawartości woluminu (w przypadku zamontowania w trybie do odczytu i zapisu).

Aby przeglądać zawartość zamontowanego woluminu, wybierz go w tabeli i kliknij  **Przeglądaj**. Pojawi się okno domyślnego menedżera plików, w którym można sprawdzić zawartość zamontowanego woluminu.

Odmontowywanie obrazów

Utrzymywanie zamontowanych woluminów wymaga dużej ilości zasobów systemowych. Zaleca się odmontowanie woluminów po wykonaniu niezbędnych operacji. Jeśli woluminy nie zostaną odmontowane ręcznie, pozostaną zamontowane do momentu ponownego uruchomienia systemu operacyjnego.

Aby odmontować obraz, wybierz go w tabeli i kliknij  **Odmontuj**.

Aby odmontować wszystkie zamontowane woluminy, kliknij  **Odmontuj wszystkie**.

7.4 Operacje dostępne w skarbcach

Użycie skarbców ułatwia dostęp do archiwów i kopii zapasowych oraz wykonywanie operacji zarządzania archiwami.

Aby wykonywać operacje dotyczące archiwów i kopii zapasowych





1. W panelu **Nawigacja** wybierz skarbiec, którego archiwami musisz zarządzać.
2. W widoku skarbcza wybierz kartę **Widok archiwum**. Prezentuje ona listę wszystkich archiwów przechowywanych w wybranym skarbcu.
3. Przejdź do czynności opisanych w sekcji
 - Operacje na archiwach (s. 245)
 - Operacje na kopiach zapasowych (s. 245)

7.4.1 Operacje na archiwach

Aby wykonać jakąkolwiek operację na archiwum

1. W panelu **Nawigacja** wybierz skarbiec zawierający archiwa.
2. Wybierz archiwum w zakładce **Widok archiwum** skarbca. Jeśli archiwum jest chronione hasłem, pojawi się monit o jego podanie.
3. Wykonuj operacje poprzez kliknięcie odpowiednich przycisków na pasku narzędzi. Dostęp do tych operacji można również uzyskać wybierając element **Czynności „[nazwa archiwum]”** w menu głównym.

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na archiwach przechowywanych w skarbcu.








Zadanie	Czynności
Sprawdzanie poprawności archiwum	<p>Kliknij  Sprawdź poprawność.</p> <p>Pojawi się strona Sprawdzanie poprawności (s. 231) ze wstępnie wybranym archiwum jako źródłem.</p> <p>Sprawdzenie poprawności archiwum oznacza sprawdzenie wszystkich kopii zapasowych w tym archiwum.</p>
Eksport archiwum	<p>Kliknij  Eksportuj.</p> <p>Pojawi się strona Eksport (s. 235) ze wstępnie wybranym archiwum jako źródłem. Eksport archiwum polega na utworzeniu w określonej lokalizacji zduplikowanego archiwum z wszystkimi kopiami zapasowymi.</p>
Usuwanie pojedynczego archiwum lub wielu archiwów	<p>1. Wybierz archiwum lub archiwa do usunięcia.</p> <p>2. Kliknij  Usuń.</p> <p>Program przedstawi dokonany wybór w oknie Usuwanie kopii zapasowej (s. 247), które zawiera pola wyboru obok każdego archiwum i każdej kopii zapasowej. Sprawdź wybrane archiwa i w razie potrzeby dokonaj zmian (zaznacz pola wyboru żądanych archiwów), a następnie potwierdź usunięcie.</p>
Usuwanie wszystkich archiwów ze skarbca	<p>Należy pamiętać, że jeśli na liście skarbców zastosowano filtry, jest widoczna tylko część zawartości skarbca. Przed rozpoczęciem operacji upewnij się, że skarbiec nie zawiera żadnych potrzebnych archiwów.</p> <p>Kliknij  Usuń wszystkie.</p> <p>Program przedstawi dokonany wybór w nowym oknie, które zawiera pola wyboru obok każdego archiwum i każdej kopii zapasowej. Sprawdź i w razie potrzeby zmień wybór, a następnie potwierdź usunięcie.</p>

7.4.2 Operacje na kopiach zapasowych

Aby wykonać jakąkolwiek operację na archiwum

1. W panelu **Nawigacja** wybierz skarbiec zawierający archiwa.
2. Wybierz archiwum w zakładce **Widok archiwum** skarbca. Następnie rozwiń archiwum i kliknij kopię zapasową, aby ją zaznaczyć. Jeśli archiwum jest chronione hasłem, pojawi się monit o jego podanie.
3. Wykonuj operacje poprzez kliknięcie odpowiednich przycisków na pasku narzędzi. Dostęp do tych operacji można również uzyskać wybierając element **Czynności „[nazwa kopii zapasowej]”** w menu głównym.

Poniżej przedstawiono wytyczne dotyczące wykonywania operacji na kopiach zapasowych.

Zadanie	Czynności
Wyświetlanie zawartości kopii zapasowej w osobnym oknie	Kliknij  Wyświetl zawartość . W oknie Zawartość kopii zapasowej sprawdź zawartość kopii zapasowej.
Odzyskiwanie	Kliknij  Odzyskaj . Zostanie otwarta strona Odzyskaj dane (s. 130) ze wstępnie wybraną kopią zapasową jako źródłem.
Konwersja kopii zapasowej woluminu lub dysku na maszynę wirtualną	Kliknij kopię zapasową prawym przyciskiem myszy, a następnie wybierz Konwertuj na maszynę wirtualną . Zostanie otwarta strona Odzyskaj dane (s. 130) ze wstępnie wybraną kopią zapasową jako źródłem. Wybierz lokalizację i typ nowej maszyny wirtualnej, a następnie wykonaj te same czynności co przy odzyskiwaniu dysku lub woluminu.
Sprawdzanie poprawności kopii zapasowej	Kliknij  Sprawdź poprawność . Pojawi się strona Sprawdzanie poprawności (s. 231) ze wstępnie wybraną kopią zapasową jako źródłem. 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.
Eksportowanie kopii zapasowej	Kliknij  Eksportuj . Pojawi się strona Eksport (s. 235) ze wstępnie wybraną kopią zapasową jako źródłem. Eksport kopii zapasowej polega na utworzeniu w wybranej lokalizacji nowego archiwum z samowystarczalną kopią zapasową.
Konwertowanie kopii zapasowej na pełną kopię zapasową	Kliknij  Konwertuj na pełną kopię zapasową , aby zastąpić przyrostową lub różnicową kopię zapasową pełną kopią obejmującą ten sam punkt w czasie. Aby uzyskać więcej informacji, zobacz „Konwertowanie na pełną kopię zapasową” (s. 246).
Usuwanie jednej lub wielu kopii zapasowych	Wybierz jedną z kopii zapasowych do usunięcia, a następnie kliknij  Usuń . Program przedstawi dokonany wybór w oknie Usuwanie kopii zapasowej (s. 247), które zawiera pola wyboru obok każdego archiwum i każdej kopii zapasowej. Sprawdź i w razie potrzeby zmień wybór (zaznacz pola wyboru żądanych kopii zapasowych), a następnie potwierdź usunięcie.
Usuwanie wszystkich archiwów i kopii zapasowych ze skarbca	Należy pamiętać, że jeśli na liście skarbów zastosowano filtry, jest widoczna tylko część zawartości skarbca. Przed rozpoczęciem operacji upewnij się, że skarbiec nie zawiera żadnych potrzebnych archiwów. Kliknij  Usuń wszystkie . Program przedstawi dokonany wybór w oknie Usuwanie kopii zapasowej (s. 247), które zawiera pola wyboru obok każdego archiwum i każdej kopii zapasowej. Sprawdź i w razie potrzeby zmień wybór, a następnie potwierdź usunięcie.

7.4.3 Konwertowanie kopii zapasowej na pełną kopię zapasową

Gdy ciąg przyrostowych kopii zapasowych w archiwum wydłuży się, konwersja kopii przyrostowej na pełną zwiększy niezawodność archiwum. Czasem warto również przeprowadzić konwersję różnicowej kopii zapasowej, jeśli są od niej zależne kopie przyrostowe.

Podczas konwersji zaznaczone kopie przyrostowe lub różnicowe są zastępowane pełną kopią zapasową obejmującą ten sam punkt w czasie. Poprzednie kopie zapasowe w ciągu nie ulegają zmianie. Są natomiast aktualizowane również wszystkie kolejne przyrostowe i różnicowe kopie zapasowe do najbliższej kopii pełnej. Najpierw są tworzone nowe wersje kopii zapasowych, a dopiero później usuwane są stare kopie. Z tego względu w lokalizacji musi być dostatecznie dużo wolnego miejsca, aby tymczasowo pomieścić zarówno stare, jak i nowe wersje kopii zapasowych.

Konwersja nie polega na utworzeniu kopii kopii zapasowej. Aby uzyskać samowystarczalną kopię kopii zapasowej na dysku flash lub nośniku wymiennym, skorzystaj z operacji export (s. 235).

Przykład

W archiwum znajduje się następujący ciąg kopii zapasowych:

F1 I2 I3 I4 D5 I6 I7 I8 F9 I10 I11 D12 F13

F oznacza pełną kopię zapasową, **I** — przyrostową, **D** — różnicową.

Konwertujesz przyrostową kopię zapasową **I4** na pełną kopię zapasową. Kopie zapasowe **I4, D5, I6, I7, I8** zostaną zaktualizowane, natomiast **I10 I11 D12** pozostaną niezmiennione, ponieważ zależą od kopii **F9**.

Ograniczenie: Operacja **Konwertuj na pełną kopię zapasową** nie jest dozwolona w przypadku kopii zapasowych na taśmach i płytach CD/DVD.

7.4.4 Usuwanie archiwów i kopii zapasowych

W oknie **Usuwanie kopii zapasowej** jest wyświetlana taka sama karta jak w widoku skarbców, ale z polami wyboru obok każdego archiwum i każdej kopii zapasowej. Obok archiwum lub kopii zapasowej wybranej do usunięcia znajduje się znacznik wyboru. Przejrzyj archiwa i kopie zapasowe wybrane do usunięcia. Aby usunąć inne archiwa i kopie zapasowe, zaznacz odpowiednie pola wyboru, a następnie kliknij **Usuń wybrane** i potwierdź usunięcie.

Co się stanie, jeśli usunę kopię zapasową, która jest podstawą przyrostowej lub różnicowej kopii zapasowej?

Aby zachować spójność archiwów, program skonsoliduje obie kopie zapasowe. Załóżmy na przykład, że usuwasz pełną kopię zapasową, ale zachowujesz następną kopię przyrostową. Kopie zapasowe zostaną połączone w jedną, pełną kopię zapasową, która zostanie usunięta w dniu zaplanowanego usunięcia przyrostowej kopii zapasowej. Po usunięciu przyrostowej lub różnicowej kopii zapasowej ze środka łańcucha wynikowa kopia zapasowa będzie kopią przyrostową.

Należy pamiętać, że konsolidacja to jedynie metoda usuwania, ale nie alternatywa do 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.

W skarbcu należy zapewnić wystarczającą ilość wolnego miejsca na pliki tymczasowe tworzone podczas konsolidacji. Kopie zapasowe otrzymane w wyniku konsolidacji zawsze mają maksymalną kompresję.

8 Nośnik startowy

Nośnik startowy

Nośnik startowy to nośnik fizyczny (płyta CD lub DVD, dysk USB albo inny nośnik obsługiwany jako urządzenie startowe w systemie BIOS komputera), który uruchamia się na dowolnym komputerze klasy PC i umożliwia uruchomienie agenta programu Acronis Backup & Recovery 11 w środowisku opartym na systemie Linux lub w środowisku preinstalacyjnym systemu Windows (WinPE) bez pomocy systemu operacyjnego. Najczęstsze zastosowanie nośnika startowego:

- odzyskiwanie systemu operacyjnego, którego nie można uruchomić;
- uzyskanie dostępu do danych ocalałych w uszkodzonym systemie i utworzenie ich kopii zapasowej;
- wdrożenie systemu operacyjnego po awarii;
- utworzenie standardowych lub dynamicznych woluminów po awarii;
- utworzenie kopii zapasowej „sektor po sektorze” dysku z nieobsługiwanym systemem plików;
- utworzenie w trybie offline kopii zapasowej wszelkich danych, których kopii zapasowej nie można utworzyć w trybie online ze względu na ograniczony dostęp, trwałą blokadę założoną przez uruchomione aplikacje lub z jakichkolwiek innych powodów.

Komputer można uruchomić w powyższych środowiskach za pomocą nośnika fizycznego albo przez sieć z serwera Acronis PXE Server, Windows Deployment Services (WDS) lub Remote Installation Services (RIS). Te serwery z przesłanymi na nie komponentami startowymi można również traktować jako swego rodzaju nośniki startowe. Za pomocą tego samego kreatora można utworzyć nośnik startowy bądź skonfigurować serwer PXE lub WDS/RIS.

Nośnik startowy oparty na systemie Linux

Nośnik oparty na systemie Linux zawiera agenta startowego Acronis Backup & Recovery 11 Bootable Agent 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. Operacje te mogą być konfigurowane i kontrolowane lokalnie lub zdalnie przy użyciu konsoli zarządzania.

Nośnik startowy oparty na środowisku PE

Nośnik startowy oparty na środowisku PE zawiera minimalną wersję systemu Windows nazywaną środowiskiem preinstalacyjnym systemu Windows (WinPE) oraz wtyczkę Acronis Plug-in for WinPE, to znaczy modyfikację agenta programu Acronis Backup & Recovery 11, która może być uruchamiana w środowisku preinstalacyjnym.

Środowisko WinPE jest najwygodniejszym rozwiązaniem startowym w dużych środowiskach wyposażonych w różnorodny sprzęt.

Zalety:

- Korzystanie z programu Acronis Backup & Recovery 11 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 programu Acronis Backup & Recovery 11, ale także poleceń i skryptów środowiska PE oraz innych dodanych do niego wtyczek.

- 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. Nośnik oparty na środowisku PE 2.x, czyli na jądrze systemu Windows Vista lub Windows Server 2008, umożliwia dynamiczne ładowanie potrzebnych sterowników urządzeń.

Ograniczenie:

Nośnik startowy oparty na środowisku PE nie obsługuje technologii UEFI.

8.1 Jak utworzyć nośnik startowy

Aby było możliwe tworzenie nośników fizycznych, komputer musi być wyposażony w nagrywarkę CD/DVD lub umożliwiać podłączenie dysku flash. Aby było możliwe konfigurowanie serwera PXE lub WDS/RIS, komputer musi być podłączony do sieci. Generator nośnika startowego umożliwia także utworzenie obrazu ISO dysku startowego, który później można będzie nagrać na czystej płycie.

Nośnik startowy oparty na systemie Linux

Uruchom Generator nośnika startowego (za pomocą konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako oddzielny komponent).

Wybierz sposób obsługi woluminów i zasobów sieciowych (tzw. styl nośników):

- Nośnik obsługujący woluminy w stylu systemu Linux wyświetla woluminy jako np. hda1 i sdb2. Przed rozpoczęciem odzyskiwania próbuje zrekonstruować urządzenia MD i woluminy logiczne (LVM).
- Nośnik obsługujący woluminy w stylu systemu Windows wyświetla woluminy jako np. C: i D:. Zapewnia dostęp do woluminów dynamicznych (LDM).

Specjalny kreator pomoże w wykonaniu niezbędnych operacji. Aby uzyskać szczegółowe informacje, zobacz Nośnik startowy oparty na systemie Linux (s. 250).

Nośnik startowy oparty na środowisku PE

Wtyczkę Acronis Plug-in for WinPE można dodać do dystrybucji środowiska WinPE opartych na dowolnym z następujących jąder:

- Windows XP Professional z dodatkiem Service Pack 2 (PE 1.5)
- Windows Server 2003 z dodatkiem Service Pack 1 (PE 1.6)
- Windows Vista (PE 2.0)
- Windows Vista SP1 i Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0)

Jeśli masz już nośnik z dystrybucją PE1.x, rozpakuj obraz ISO nośnika do folderu lokalnego i uruchom Generator nośnika startowego z konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako osobny komponent. Specjalny kreator pomoże w wykonaniu niezbędnych operacji. Aby uzyskać szczegółowe informacje, zobacz Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 1.x (s. 255).

Aby umożliwić tworzenie i modyfikowanie obrazów środowiska PE 2.x lub 3.0, należy zainstalować Generator nośnika startowego na komputerze, na którym jest zainstalowany zestaw zautomatyzowanej instalacji systemu Windows (Windows AIK). Dalsze operacje opisano w sekcji Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 2.x lub 3.0 (s. 255).

Jeśli na komputerze nie jest zainstalowany zestaw Windows AIK, przygotuj się w następujący sposób:

1. Pobierz i zainstaluj zestaw zautomatyzowanej instalacji systemu Windows.

Zestaw zautomatyzowanej instalacji systemu Windows Vista (PE 2.0):

<http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=pl>

Zestaw zautomatyzowanej instalacji systemów Windows Vista SP1 i Windows Server 2008 (PE 2.1):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=pl>

Zestaw zautomatyzowanej instalacji systemu Windows 7 (PE 3.0):

<http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=pl>

Wymagania systemowe dotyczące instalacji można znaleźć, korzystając z powyższych łączy.

2. [Opcjonalnie] Nagraj zestaw zautomatyzowanej instalacji systemu Windows na płycie DVD lub skopiuj go na dysk flash.
3. Zainstaluj środowisko Microsoft .NET Framework 2.0 zawarte w tym zestawie (NETFXx86 lub NETFXx64, w zależności od posiadanego sprzętu).
4. Zainstaluj analizator Microsoft Core XML (MSXML) 5.0 lub 6.0 zawarty w tym zestawie.
5. Zainstaluj zestaw zautomatyzowanej instalacji systemu Windows zawarty w tym zestawie.
6. Zainstaluj Generator nośnika startowego na tym samym komputerze.

Zalecamy zapoznanie się z dokumentacją pomocy dostarczoną z zestawem zautomatyzowanej instalacji systemu Windows. Aby uzyskać dostęp do dokumentacji, z menu Start wybierz **Microsoft Windows AIK -> Dokumentacja**.

Korzystanie ze środowiska Bart PE

Używając generatora Bart PE Builder, można utworzyć obraz środowiska Bart PE z wtyczką Acronis Plug-in. Aby uzyskać szczegółowe informacje, zobacz Generowanie środowiska Bart PE z wtyczką Acronis Plug-in z dystrybucji systemu Windows (s. 257).

8.1.1 Nośnik startowy oparty na systemie Linux

W przypadku korzystania z generatora nośnika należy określić następujące elementy:

1. [Opcjonalnie] Parametry jądra systemu Linux. Kolejne parametry należy oddzielać spacjami. Aby móc wybrać tryb wyświetlania agenta startowego przy każdym uruchomieniu nośnika, należy wpisać **vga=ask**. Lista parametrów znajduje się w sekcji Parametry jądra (s. 251).
2. Komponenty startowe Acronis, które zostaną umieszczone na nośniku. Jeśli na komputerze, na którym jest tworzony nośnik, zainstalowano dodatek Acronis Backup & Recovery 11 Universal Restore, zostanie on włączony.
3. [Opcjonalnie] Wartość limitu czasu menu startowego oraz komponent, który będzie automatycznie uruchamiany po przekroczeniu tego limitu.
 - Jeśli ta opcja nie zostanie skonfigurowana, program ładujący Acronis będzie czekał, aż użytkownik określi, czy ma być uruchamiany system operacyjny (jeśli istnieje), czy komponent Acronis.

- Jeśli ustawisz na przykład **10 s** dla agenta startowego, agent zostanie uruchomiony po upływie 10 s od wyświetlenia menu. Umożliwia to wykonanie nienadzorowanych operacji lokalnych podczas uruchamiania z serwera PXE lub WDS/RIS.
4. [Opcjonalnie] Ustawienia zdalnego logowania:
 - Nazwa użytkownika i hasło, które należy wprowadzić po stronie konsoli podczas nawiązywania połączenia z agentem. Jeśli te pola pozostaną puste, połączenie będzie włączane po wpisaniu dowolnych symboli w oknie monitu.
 5. [Opcjonalnie] Ustawienia sieciowe (s. 253):
 - Ustawienia TCP/IP, które zostaną przypisane do kart sieciowych komputera.
 6. [Opcjonalnie] Port sieciowy (s. 254):
 - Port TCP, na którym agent startowy nasłuchuje połączeń przychodzących.
 7. Typ nośnika do utworzenia. Można:
 - utworzyć płytę CD lub DVD albo inny nośnik startowy, na przykład wymienny dysk flash USB, jeśli system BIOS umożliwia uruchamianie komputera z tego rodzaju nośników;
 - wygenerować obraz ISO dysku startowego, który później można będzie nagrać na czystej płycie;
 - przesłać wybrane komponenty na serwer Acronis PXE Server;
 - przesłać wybrane komponenty na serwer WDS/RIS.
 8. [Opcjonalnie] Sterowniki systemu Windows, które będą używane przez dodatek Acronis Universal Restore. (s. 254) To okno jest wyświetlane tylko w przypadku, gdy zainstalowano dodatek Acronis Universal Restore i wybrano nośnik inny niż serwer PXE lub WDS/RIS.
 9. Ścieżka do pliku ISO nośnika bądź nazwa lub adres IP i poświadczenia serwera PXE lub WDS/RIS.

Parametry jądra

To okno pozwala określić parametry jądra systemu Linux. Zostaną one automatycznie zastosowane po uruchomieniu nośnika startowego.

Parametry te są przeważnie używane w razie problemów z pracą z nośnika startowego. W standardowych sytuacjach pole to może pozostać puste.

Każdy z wpisywanych parametrów można także podać, naciskając przy starcie systemu klawisz F11.

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.

vga=numer_trybu

Określa trybu obrazu używanego przez graficzny interfejs użytkownika nośnika startowego. Numer trybu jest określony wartością *numer_trybu* podaną w formacie szesnastkowym, na przykład **vga=0x318**

Rozdzielczość ekranu i liczba kolorów w wybranym trybie może zależeć od komputera. Aby wybrać odpowiednią wartość **numer_trybu**, zaleca się najpierw użycie parametru *vga=ask*.

quiet

Wyłącza wyświetlanie komunikatów startowych podczas ładowania jądra systemu Linux, a po jego załadowaniu uruchamia konsolę zarządzania.

Parametr ten jest pośrednio określony podczas tworzenia nośnika startowego, jednak w menu startowym można go usunąć.

Bez tego parametru zostaną wyświetlone wszystkie komunikaty startowe, a następnie pojawi się wiersz poleceń. Aby uruchomić z niego konsolę zarządzania, wpisz 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 rozpoznawanie urządzeń PCMCIA.

nomouse

Wyłącza obsługę myszy.

nazwa_modułu=off

Wyłącza moduł określony w parametrze *nazwa_modułu*. Aby na przykład wyłączyć obsługę modułu SATA, określ **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

Uzyskuje tabelę przekierowywania przerw za pomocą wywołań systemu BIOS interfejsu PCI. Użyj tego parametru, jeśli jądro nie może przydzielić żądań przerw (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 przerw.

Ustawienia sieciowe

Podczas tworzenia nośnika startowego Acronis można wstępnie skonfigurować połączenia sieciowe, których będzie używał agent startowy. Można wstępnie skonfigurować następujące parametry:

- adres IP,
- maska podsieci,
- brama,
- serwer DNS,
- serwer WINS.

Gdy agent startowy uruchamia się na komputerze, konfiguracja jest stosowana do karty interfejsu sieciowego (NIC) komputera. Jeśli ustawienia nie zostały wstępnie skonfigurowane, agent używa automatycznej konfiguracji DHCP. Ustawienia sieciowe można także skonfigurować ręcznie, gdy agent startowy jest uruchomiony na komputerze.

Wstępne konfigurowanie wielu połączeń sieciowych

Można wstępnie skonfigurować ustawienia TCP/IP dla maksymalnie dziesięciu kart interfejsu sieciowego. Aby zagwarantować przypisanie odpowiednich ustawień do każdej karty, należy utworzyć nośnik na serwerze, do którego zostanie on dostosowany. Po wybraniu istniejącej karty interfejsu sieciowego w oknie kreatora zostaną zaznaczone jej ustawienia, które zostaną zapisane na nośniku. Na nośniku zostanie także zapisany adres MAC każdej istniejącej karty interfejsu sieciowego.

Ustawienia, z wyjątkiem adresu MAC, można zmienić. Jeśli istnieje taka potrzeba, można także skonfigurować ustawienia nieistniejącej karty interfejsu sieciowego.

Gdy agent startowy uruchamia się na serwerze, pobiera listę dostępnych kart interfejsu sieciowego. Lista jest posortowana według gniazd zajmowanych przez karty: karta znajdująca się najbliżej procesora jest wyświetlana na górze listy.

Agent startowy przypisuje do każdej znanej karty interfejsu sieciowego odpowiednie ustawienia, identyfikując karty na podstawie ich adresów MAC. Po skonfigurowaniu kart interfejsu sieciowego o znanych adresach MAC do pozostałych kart są przypisywane ustawienia, które zostały wprowadzone dla nieistniejących kart, poczynawszy od najwyższej nieprzypisanej karty interfejsu sieciowego.

Nośnik startowy można dostosować do dowolnego komputera, a nie tylko do komputera, na którym został utworzony. Aby to zrobić, należy skonfigurować karty interfejsu sieciowego zgodnie z kolejnością ich gniazd na tym komputerze: NIC1 zajmuje gniazdo najbliższe procesora, w następnym gnieździe znajduje się NIC2 itd. Gdy agent startowy będzie uruchamiał się na tym komputerze, nie znajdzie żadnych kart o znanych adresach MAC i skonfiguruje karty w takiej samej kolejności jak użytkownik.

Przykład

Agent startowy może używać jednej z kart sieciowych do komunikacji z konsolą zarządzania przez sieć produkcyjną. Na potrzeby tego połączenia można utworzyć konfigurację automatyczną. Duże ilości

danych odzyskiwania można przesyłać za pośrednictwem drugiej karty, uwzględnionej w dedykowanej sieci tworzenia kopii zapasowych za pomocą ustawień statycznego adresu TCP/IP.

Port sieciowy

Podczas tworzenia nośnika startowego można wstępnie skonfigurować port sieciowy, na którym będzie nasłuchiwał agent startowy, aby uzyskać informacje o połączeniu przychodzącym. Dostępne opcje to:

- port domyślny,
- aktualnie używany port,
- nowy port (należy wprowadzić numer portu).

Jeśli port nie został wstępnie skonfigurowany, agent używa domyślnego numeru portu (9876). Ten port jest także używany domyślnie przez konsolę zarządzania Acronis Backup & Recovery 11 Management Console.

Sterowniki dodatku Universal Restore

Podczas tworzenia nośnika startowego można dodać do nośnika sterowniki systemu Windows. Sterowniki będą używane przez dodatek Universal Restore podczas odzyskiwania systemu Windows na komputerze z innym procesorem, inną płytą główną lub innym urządzeniem pamięci masowej niż w systemie, którego kopia zapasowa została utworzona.

Dodatek Universal Restore można skonfigurować:

- aby wyszukiwać na nośniku sterowniki, które najlepiej pasują do sprzętu docelowego;
- aby pobierać z nośnika jawnie określone sterowniki pamięci masowej. Jest to konieczne, gdy sprzęt docelowy jest wyposażony w określony kontroler pamięci dyskowej masowej (na przykład kartę SCSI, RAID lub Fiber Channel).

Aby uzyskać więcej informacji, zobacz Universal Restore.

Sterowniki zostaną umieszczone w widocznym folderze Drivers na nośniku startowym. Sterowniki nie są ładowane do pamięci RAM komputera docelowego, dlatego w czasie pracy dodatku Universal Restore nośnik musi być włożony lub podłączony.

Dodawanie sterowników do nośnika startowego jest dostępne pod warunkiem, że:

1. na komputerze, na którym jest tworzony nośnik startowy, zainstalowano dodatek Acronis Backup & Recovery 11 Universal Restore; ORAZ
2. użytkownik tworzy nośnik wymienny, jego obraz ISO lub nośnik odłączany, taki jak dysk flash. Nie można przesłać sterowników na serwer PXE ani WDS/RIS.

Sterowniki można dodawać do listy wyłącznie w grupach, dodając pliki INF lub foldery zawierające takie pliki. Nie można wybierać pojedynczych sterowników z plików INF, ale generator nośnika pokazuje zawartość pliku dla celów informacyjnych.

Aby dodać sterowniki:

1. Kliknij **Dodaj** i znajdź plik INF lub folder zawierający pliki INF.
2. Wybierz plik INF lub folder.
3. Kliknij **OK**.

Sterowniki można usuwać z listy wyłącznie w grupach, usuwając pliki INF.

Aby usunąć sterowniki:

1. Wybierz plik INF.

2. Kliknij **Usuń**.

8.1.2 Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 1.x

Wtyczkę Acronis Plug-in for WinPE można dodać do środowiska:

- Windows PE 2004 (1.5) (system Windows XP Professional z dodatkiem Service Pack 2),
- Windows PE 2005 (1.6) (system Windows Server 2003 z dodatkiem Service Pack 1).

Aby dodać wtyczkę Acronis Plug-in do środowiska WinPE 1.x:

1. Rozpakuj wszystkie pliki z obrazu ISO środowiska WinPE 1.x do oddzielnego folderu na dysku twardym.
2. Uruchom Generator nośnika startowego (za pomocą konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako oddzielny komponent).
3. Wybierz **Typ nośnika startowego: Windows PE**.
 - Wybierz polecenie **Użyj plików WinPE znajdujących się w określonym folderze**.
4. Określ ścieżkę do folderu zawierającego pliki WinPE.
5. Określ ustawienia sieciowe (s. 253) kart sieciowych komputera lub wybierz automatyczną konfigurację DHCP.
6. Określ pełną ścieżkę do wynikowego pliku ISO, łącznie z nazwą pliku.
7. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.
8. Nagraj obraz ISO na płycie CD lub DVD za pomocą narzędzia innej firmy albo skopiuj obraz na dysk flash.

Po uruchomieniu komputera w środowisku WinPE automatycznie uruchomi się program Acronis Backup & Recovery 11.

8.1.3 Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 2.x lub 3.0

Generator nośnika startowego oferuje trzy metody integracji programu Acronis Backup & Recovery 11 ze środowiskiem WinPE 2.x lub 3.0:

- dodanie wtyczki Acronis Plug-in do istniejącego obrazu ISO środowiska PE — możliwość przydatna, gdy wtyczkę trzeba dodać do wcześniej skonfigurowanego i już używanego obrazu ISO środowiska PE;
- utworzenie od podstaw obrazu ISO środowiska PE z wtyczką;
- dodanie wtyczki Acronis Plug-in do pliku WIM do dowolnych przyszłych celów (ręczne generowanie obrazu ISO, dodawanie innych narzędzi do obrazu itd.).

Aby umożliwić wykonanie dowolnej z tych operacji, należy zainstalować Generator nośnika startowego na komputerze, na którym jest zainstalowany zestaw zautomatyzowanej instalacji systemu Windows. Jeśli taki komputer nie istnieje, należy przygotować go w sposób opisany w sekcji Jak utworzyć nośnik startowy (s. 249).

Generator nośnika startowego obsługuje tylko środowisko WinPE 2.x lub 3.0 x86. Te dystrybucje środowiska WinPE mogą także działać na sprzęcie o architekturze x64.

Obrazy PE oparte na środowisku Win PE 2.x lub 3.0 wymagają co najmniej 640 MB pamięci RAM.

Dodawanie wtyczki Acronis Plug-in do obrazu ISO środowiska WinPE 2.x lub 3.0

Aby dodać wtyczkę Acronis Plug-in do obrazu ISO środowiska WinPE 2.x lub 3.0:

1. W przypadku dodawania wtyczki do istniejącego obrazu ISO środowiska Win PE należy rozpakować wszystkie pliki tego obrazu do oddzielnego folderu na dysku twardym.
2. Uruchom Generator nośnika startowego (za pomocą konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako oddzielny komponent).
3. Wybierz **Typ nośnika startowego: Windows PE**.

W przypadku tworzenia nowego obrazu ISO środowiska PE:

- Wybierz **Utwórz automatycznie środowisko Windows PE 2.x lub 3.0**.
- Program uruchomi odpowiedni skrypt i przejdzie do następnego okna.

W trakcie dodawania wtyczki do istniejącego obrazu ISO środowiska PE:

- Wybierz polecenie **Użyj plików WinPE znajdujących się w określonym folderze**.
- Określ ścieżkę do folderu zawierającego pliki WinPE.

4. Określ ustawienia sieciowe (s. 253) kart sieciowych komputera lub wybierz automatyczną konfigurację DHCP.
5. [Opcjonalnie] Określ sterowniki systemu Windows, które mają być dodane do środowiska Windows PE. Po uruchomieniu komputera w środowisku Windows PE sterowniki ułatwiają dostęp do urządzenia, na którym znajduje się archiwum kopii zapasowej. Sterowniki te można również wskazać podczas konfiguracji komponentu Universal Restore. Samo środowisko WinPE wymaga sterowników 32-bitowych. Aby móc korzystać z komponentu Universal Restore w systemie 64-bitowym, dodaj również sterowniki 64-bitowe.
Kliknij **Dodaj** i określ ścieżkę do niezbędnego pliku *.inf dla odpowiedniego kontrolera SCSI, RAID, SATA, karty sieciowej, napędu taśmowego lub innego urządzenia. Procedurę tę należy powtórzyć w przypadku każdego sterownika, który ma być dołączony do wynikowego nośnika startowego środowiska WinPE.
6. Wybierz, czy chcesz utworzyć obraz ISO lub WIM czy przesłać nośnik na serwer (Acronis PXE Server, WDS lub RIS).
7. Określ pełną ścieżkę do wynikowego pliku obrazu (włącznie z nazwą pliku) lub określ serwer i podaj nazwę użytkownika i hasło, aby uzyskać do niego dostęp.
8. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.
9. Nagraj obraz ISO na płycie CD lub DVD za pomocą narzędzia innej firmy albo skopiuj obraz na dysk flash.

Po uruchomieniu komputera w środowisku WinPE automatycznie uruchomi się program Acronis Backup & Recovery 11.

Aby utworzyć obraz środowiska PE (plik ISO) z wynikowego pliku WIM:

- Zastąp domyślny plik boot.wim w folderze Windows PE nowo utworzonym plikiem WIM. W powyższym przykładzie wpisz:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Używanie narzędzia **Oscdimg**. W powyższym przykładzie wpisz:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO  
c:\winpe_x86\winpe_x86.iso
```

Aby uzyskać więcej informacji na temat dostosowywania środowiska Windows PE, zobacz Windows Preinstallation Environment User's Guide (Podręcznik użytkownika środowiska preinstalacyjnego systemu Windows) (Winpe.chm).

8.1.4 Generowanie środowiska Bart PE z wtyczką Acronis Plug-in z dystrybucji systemu Windows

1. Uzyskaj generator środowiska Bart PE.
2. Zainstaluj Generator nośnika startowego z pliku instalacyjnego programu Acronis Backup & Recovery 11.
3. Zmień bieżący folder na folder, w którym jest zainstalowana wtyczka Acronis Plug-in for WinPE — domyślnie: C:\Program Files\Acronis\Bootable Components\WinPE.
Jeśli wtyczka jest zainstalowana w folderze innym niż domyślny, zmień odpowiednio ścieżkę (aby poznać lokalizację wtyczki, sprawdź klucz rejestru HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Bootable Components\Settings\WinPE).
4. Rozpakuj plik WinPE.zip do bieżącego folderu.
5. Uruchom następujące polecenie:

```
make_plugin.vbs
```

W wyniku działania tej operacji folder o nazwie **acronis** zostanie utworzony w katalogu bieżącym.
6. Skopiuj folder **acronis** do folderu %BartPE folder%\plugins.
7. Jeśli na dysku twardym nie ma kopii plików instalacyjnych systemu Windows, włóż płytę CD z dystrybucją tego systemu.
8. Uruchom generator środowiska Bart PE.
9. Określ ścieżkę do plików instalacyjnych systemu Windows lub płyty CD z dystrybucją systemu Windows.
10. Kliknij **Plugins** (Wtyczki) i sprawdź, czy jest włączona wtyczka programu Acronis Backup & Recovery 11. Jeśli jest wyłączona, włącz ją.
11. Określ folder wyjściowy i pełną ścieżkę do wynikowego pliku ISO, włącznie z nazwą pliku lub nośnikiem do utworzenia.
12. Wygeneruj środowisko Bart PE.
13. Nagraj obraz ISO na płycie CD lub DVD (jeśli jeszcze nie zostało to zrobione) lub skopiuj go na dysk flash.

Po uruchomieniu komputera w środowisku Bart PE i skonfigurowaniu połączenia sieciowego wybierz **Go -> System -> Storage -> Acronis Backup & Recovery 11** (Przejdź -> System -> Magazyn -> Acronis <PRODUCT NAME>) w celu rozpoczęcia pracy.

8.2 Łączenie z komputerem uruchamianym z nośnika

Po uruchomieniu komputera z nośnika startowego terminal komputera wyświetla okno uruchamiania z adresami IP uzyskanymi z serwera DHCP lub ustawionymi zgodnie ze wstępnie skonfigurowanymi wartościami.

Połączenie zdalne

Aby podłączyć komputer zdalnie, należy wybrać **Połącz -> Zarządzaj komputerem zdalnym** w menu konsoli i określić jeden z adresów IP komputera. Należy także podać nazwę użytkownika i hasło, jeśli zostały one skonfigurowane podczas tworzenia nośnika startowego.

Połączenie lokalne

Na nośniku startowym zawsze jest obecna konsola Acronis Backup & Recovery 11 Management Console. Każdy użytkownik, który ma fizyczny dostęp do terminalu komputera, może uruchomić

konsolę i nawiązać połączenie. Wystarczy kliknąć **Uruchom konsolę zarządzania** w oknie uruchamiania agenta startowego.

8.3 Praca na nośniku startowym

Operacje wykonywane na komputerze uruchamianym za pomocą nośnika startowego są bardzo podobne do operacji tworzenia kopii zapasowych i odzyskiwania w systemie operacyjnym. Różnice są następujące:

1. Litera dysków widoczne podczas pracy z nośnikiem startowym w stylu systemu Windows mogą różnić się od sposobu identyfikacji dysków przez system Windows. Na przykład dysk D: w narzędziu ratunkowym może odpowiadać dysкови E: w systemie Windows.

Ostrożnie! Dla bezpieczeństwa zaleca się przypisywanie unikatowych nazw woluminów.

2. Na nośniku startowym w stylu systemu Linux dyski i woluminy lokalne są pokazywane jako odmontowane (sda1, sda2...).
3. Kopie zapasowe tworzone za pomocą nośników startowych charakteryzują się uproszczonym nazewnictwem plików (s. 70). Nazwy standardowe są im nadawane tylko w przypadku, gdy są one dodawane do istniejącego archiwum ze standardowym nazewnictwem plików lub gdy lokalizacja docelowa nie obsługuje uproszczonych nazw.
4. Nośnik startowy w stylu systemu Linux nie może zapisać kopii zapasowej na woluminie sformatowanym w systemie NTFS. W razie potrzeby należy przełączyć się na styl Windows.
5. Aby przełączać nośnik startowy między stylami Linux i Windows, wybierz **Narzędzia > Zmień reprezentację woluminu**.
6. W graficznym interfejsie użytkownika nośnika nie ma drzewa **Nawigacja**. Do przechodzenia między widokami służy element menu **Nawigacja**.
7. Nie można planować zadań. Tak naprawdę w ogóle nie można tworzyć zadań. Jeśli trzeba powtórzyć operację, należy skonfigurować ją od początku.
8. Czas życia dziennika jest ograniczony do bieżącej sesji. Cały dziennik lub odfiltrowane wpisy dziennika można zapisać w pliku.
9. Skarbce centralne nie są wyświetlane w drzewie folderów okna **Archiwum**.

Aby uzyskać dostęp do skarbca zarządzanego, w polu **Ścieżka** wpisz następujący ciąg:

bsp://adres_węzła/nazwa_skarbca/

Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.

Po wprowadzeniu poświadczeń dostępu zostanie wyświetlona lista archiwów znajdujących się w skarbcu.

8.3.1 Konfigurowanie trybu wyświetlania

W przypadku komputera uruchamianego z nośnika tryb wyświetlania obrazu wideo jest wykrywany automatycznie na podstawie konfiguracji sprzętowej (parametrów monitora i karty graficznej). Jeśli z jakiegoś powodu tryb wideo jest wykrywany niepoprawnie, wykonaj następujące czynności:

1. W menu startowym naciśnij F11.
2. Wstaw w wierszu polecenia następujące polecenie: **vga=ask**, a następnie kontynuuj uruchamianie.
3. Z listy obsługiwanych trybów wideo wybierz odpowiedni tryb, wpisując jego numer (na przykład **318**), a następnie naciśnij ENTER.

Jeśli nie chcesz wykonywać tej procedury przy każdym uruchamianiu danej konfiguracji sprzętowej z nośnika startowego, ponownie utwórz nośnik, wprowadzając odpowiedni numer trybu (w tym przykładzie — **vga=0x318**) w oknie **Parametry jądra** (szczegółowe informacje znajdują się w sekcji Generator nośnika startowego (s. 250)).

8.3.2 Konfigurowanie urządzeń iSCSI i NDAS

W tej sekcji znajduje się opis konfigurowania urządzeń iSCSI i NDAS podczas pracy z nośnikiem startowym.

Urządzenia te są podłączane do komputera przez interfejs sieciowy i wyglądają jak urządzenia podłączane lokalnie. Urządzenia iSCSI są w sieci rozpoznawane po swoich adresach IP, a urządzenia NDAS — po identyfikatorach.

Urządzenia iSCSI są czasami nazywane obiektami docelowymi iSCSI. Komponent sprzętowy lub programowy, który zapewnia interakcję między komputerem i obiektem docelowym iSCSI, nazywany jest inicjatorem iSCSI. Nazwa inicjatora iSCSI jest z reguły definiowana przez administratora serwera, który służy jako host urządzenia.

Aby dodać urządzenie iSCSI

1. Z nośnika startowego (opartego na systemie Linux lub środowisku PE) uruchom konsolę zarządzania.
2. Kliknij **Skonfiguruj urządzenia iSCSI/NDAS** (w przypadku nośnika opartego na systemie Linux) lub **Uruchom konfigurację iSCSI** (w przypadku nośnika opartego na środowisku PE).
3. Określ adres IP i port hosta urządzenia iSCSI oraz nazwę inicjatora iSCSI.
4. Jeśli host wymaga uwierzytelniania, określ odpowiednią nazwę użytkownika i hasło.
5. Kliknij **OK**.
6. Wybierz urządzenie iSCSI z listy i kliknij **Połącz**.
7. Jeśli pojawi się monit, określ nazwę użytkownika i hasło umożliwiające dostęp do urządzenia iSCSI.

Aby dodać urządzenie NDAS

1. Z nośnika startowego opartego na systemie Linux uruchom konsolę zarządzania.
2. Kliknij **Skonfiguruj urządzenia iSCSI/NDAS**.
3. W sekcji **Urządzenia NDAS** kliknij **Dodaj urządzenie**.
4. Określ 20-znakowy identyfikator urządzenia.
5. Jeśli chcesz umożliwić zapis danych w urządzeniu, podaj pięciznakowy klucz zapisu. Bez tego klucza urządzenie będzie dostępne w trybie tylko do odczytu.
6. Kliknij **OK**.

8.4 Lista poleceń i narzędzi dostępnych na nośniku startowym opartym na systemie Linux

Nośnik startowy oparty na systemie Linux zawiera poniższe polecenia i narzędzia wiersza poleceń, których można używać po uruchomieniu powłoki poleceń. Aby uruchomić powłokę poleceń, w konsoli zarządzania nośnika startowego naciśnij klawisze CTRL+ALT+F2.

Narzędzia wiersza polecenia w oprogramowaniu Acronis

- `acrocnd`

- `acronis`
- `asamba`
- `lash`

Polecenia i narzędzia systemu Linux

<code>busybox</code>	<code>ifconfig</code>	<code>rm</code>
<code>cat</code>	<code>init</code>	<code>rmmod</code>
<code>cdrecord</code>	<code>insmod</code>	<code>route</code>
<code>chmod</code>	<code>iscsiadm</code>	<code>scp</code>
<code>chown</code>	<code>kill</code>	<code>scsi_id</code>
<code>chroot</code>	<code>kpartx</code>	<code>sed</code>
<code>cp</code>	<code>ln</code>	<code>sg_map26</code>
<code>dd</code>	<code>ls</code>	<code>sh</code>
<code>df</code>	<code>lspci</code>	<code>sleep</code>
<code>dmesg</code>	<code>lvm</code>	<code>ssh</code>
<code>dmraid</code>	<code>mdadm</code>	<code>sshd</code>
<code>e2fsck</code>	<code>mkdir</code>	<code>strace</code>
<code>e2label</code>	<code>mke2fs</code>	<code>swapoff</code>
<code>echo</code>	<code>mknod</code>	<code>swapon</code>
<code>egrep</code>	<code>mkswap</code>	<code>sysinfo</code>
<code>fdisk</code>	<code>more</code>	<code>tar</code>
<code>fsck</code>	<code>mount</code>	<code>tune2fs</code>
<code>fxload</code>	<code>mtx</code>	<code>udev</code>
<code>gawk</code>	<code>mv</code>	<code>udevinfo</code>
<code>gpm</code>	<code>pccardctl</code>	<code>udevstart</code>
<code>grep</code>	<code>ping</code>	<code>umount</code>
<code>growisofs</code>	<code>pktsetup</code>	<code>uuidgen</code>
<code>grub</code>	<code>poweroff</code>	<code>vconfig</code>
<code>gunzip</code>	<code>ps</code>	<code>vi</code>
<code>halt</code>	<code>raidautorun</code>	<code>zcat</code>
<code>hexdump</code>	<code>readcd</code>	
<code>hotplug</code>	<code>reboot</code>	

8.5 Acronis Startup Recovery Manager

Program Acronis Startup Recovery Manager to zmodyfikowana wersja agenta startowego (s. 376), znajdująca się na dysku systemowym systemu Windows lub partycji /boot systemu Linux i uruchamiana po naciśnięciu klawisza F11 podczas uruchamiania komputera. Eliminuje on potrzebę użycia oddzielnego nośnika lub połączenia sieciowego w celu uruchomienia ratunkowego narzędzia startowego.

Acronis Startup Recovery Manager jest szczególnie przydatny dla użytkowników urządzeń przenośnych. W razie awarii należy ponownie uruchomić komputer, poczekać na wyświetlenie monitu „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager...” i nacisnąć klawisz F11. Program zostanie uruchomiony i będzie można przeprowadzić odzyskiwanie.

Ponadto podczas podróży można używać funkcji Acronis Startup Recovery Manager do tworzenia kopii zapasowych.

Na komputerach z zainstalowanym programem ładującym GRUB należy wybrać funkcję Acronis Startup Recovery Manager z menu startowego, a nie naciskać klawisza F11.

Aktywuj

Aktywacja włącza monit startowy „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager” (jeśli nie ma programu ładującego GRUB) lub dodaje element „Acronis Startup Recovery Manager” do menu programu GRUB (jeśli program ten jest zainstalowany).

Aktywacja programu Acronis Startup Recovery Manager. wymaga przynajmniej 100 MB wolnego miejsca na dysku systemowym (lub na partycji /boot w systemie Linux).

Jeśli nie jest używany program ładujący GRUB zainstalowany w głównym rekordzie rozruchowym (MBR), program Acronis Startup Recovery Manager podczas aktywacji zastępuje rekord MBR własnym kodem startowym. Dlatego konieczna może być ponowna aktywacja programów ładujących innych producentów, jeśli są one zainstalowane.

Jeśli w systemie Linux jest używany inny program ładujący niż GRUB (na przykład LILO), warto przed aktywacją funkcji Acronis Startup Recovery Manager zainstalować program ładujący w rekordzie startowym partycji root (czyli rozruchowej) systemu Linux, a nie w głównym rekordzie startowym. W przeciwnym razie należy ponownie skonfigurować program ładujący po aktywacji.

Nie aktywuj

Wyłącza monit startowy „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager” (lub odpowiedni element menu w programie GRUB). Jeśli program Acronis Startup Recovery Manager jest wyłączony, a system nie uruchomi się, w celu odzyskania systemu należy wykonać jedną z poniższych czynności:

- uruchomić komputer przy użyciu oddzielnego ratunkowego nośnika startowego,
- użyć funkcji uruchamiania przez sieć z serwera Acronis PXE Server lub za pomocą usługi instalacji zdalnej (RIS) firmy Microsoft.

8.6 Acronis PXE Server

Serwer Acronis PXE Server umożliwia uruchamianie komputerów do komponentów startowych Acronis przez sieć.

Uruchomienie przez sieć:

- eliminuje potrzebę obecności technika w miejscu instalacji nośnika startowego w systemie, który musi zostać uruchomiony;
- w czasie operacji grupowych skraca czas potrzebny do uruchomienia wielu komputerów (w porównaniu z korzystaniem z fizycznego nośnika startowego).

Komponenty startowe są przesyłane na serwer Acronis PXE Server przy użyciu generatora nośnika startowego Acronis Bootable Media Builder. Aby przesłać komponenty startowe, uruchom Generator nośnika startowego (za pomocą konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako oddzielny komponent) i wykonaj szczegółowe instrukcje opisane w sekcji „Generator nośnika startowego (s. 250)”.

Uruchamianie wielu komputerów z serwera Acronis PXE Server ma sens, jeśli w sieci znajduje się serwer DHCP (Dynamic Host Control Protocol). Dzięki niemu interfejsy sieciowe uruchamianych komputerów automatycznie uzyskują adresy IP.

Ograniczenie:

Serwer Acronis PXE Server nie obsługuje programu ładującego UEFI.

8.6.1 Instalacja serwera Acronis PXE Server

Aby zainstalować serwer Acronis PXE Server:

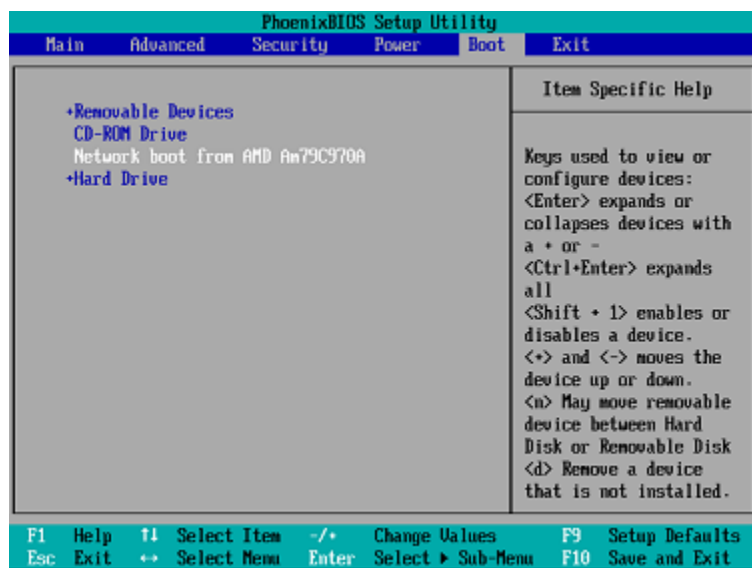
1. Uruchom plik instalacyjny programu Acronis Backup & Recovery 11.
2. Z listy **Komponenty do zarządzania scentralizowanego** wybierz serwer Acronis PXE Server.
3. Postępuj zgodnie z wyświetlanymi instrukcjami.

Serwer Acronis PXE Server uruchamia się jako usługa natychmiast po zainstalowaniu. W późniejszym czasie uruchamia się automatycznie przy każdym ponownym uruchomieniu systemu. Serwer Acronis PXE Server można zatrzymywać i uruchamiać w taki sam sposób jak inne usługi systemu Windows.

8.6.2 Konfigurowanie komputera na potrzeby uruchamiania z serwera PXE

W przypadku systemu odzyskanego po awarii wystarczy, że system BIOS komputera obsługuje uruchamianie przez sieć.

Na komputerze z systemem operacyjnym na dysku twardym należy skonfigurować system BIOS tak, aby karta interfejsu sieciowego była pierwszym urządzeniem startowym lub przynajmniej urządzeniem uruchamianym przed dyskiem twardym. Poniższy przykład przedstawia jedną z właściwych konfiguracji systemu BIOS. Jeśli do komputera nie zostanie włożony nośnik startowy, komputer uruchomi się z sieci.



W niektórych wersjach systemu BIOS po włączeniu karty interfejsu sieciowego należy zapisać zmiany, aby karta pojawiła się na liście urządzeń startowych.

Jeśli komputer jest wyposażony w wiele kart interfejsu sieciowego, należy się upewnić, że do karty obsługiwanej przez system BIOS podłączono kabel sieciowy.

8.6.3 Praca w podsięciach

Aby umożliwić pracę serwera Acronis PXE Server w innej podsięci (przez przełącznik), należy skonfigurować przełącznik tak, aby przekazywał ruch na serwerze PXE. Adresy IP serwera PXE są konfigurowane na bazie interfejsów przy użyciu funkcji pomocnika IP w taki sam sposób jak adresy serwera DHCP. Aby uzyskać więcej informacji, zobacz: <http://support.microsoft.com/kb/257579/pl>.

9 Zarządzanie dyskami

Acronis Disk Director Lite to narzędzie, które umożliwia przygotowanie konfiguracji dysków/woluminów komputera na potrzeby odzyskiwania obrazów woluminów zapisanych przez program Acronis Backup & Recovery 11.

Czasami po utworzeniu kopii zapasowej woluminu i umieszczeniu jego obrazu w bezpiecznym miejscu przechowywania konfiguracja dysków komputera może ulec zmianie z powodu wymiany dysku twardego lub utraty sprzętu. W takim przypadku za pomocą narzędzia Acronis Disk Director Lite można odtworzyć niezbędną konfigurację dysków. Pozwala to odzyskać obraz woluminu dokładnie w takiej postaci, jaką miał on wcześniej, lub wprowadzić dowolną niezbędną zmianę struktury dysków lub woluminów.

Wszystkie operacje na dyskach i woluminach wiążą się z pewnym ryzykiem uszkodzenia danych. Operacje na woluminach systemowych, startowych lub woluminach danych należy wykonywać bardzo ostrożnie, aby uniknąć możliwych problemów z procesem uruchamiania lub przechowywaniem danych na dysku twardym.

Operacje na dyskach twardych i woluminach zajmują trochę czasu, a każda przerwa w zasilaniu, niezamierzone wyłączenie komputera lub przypadkowe naciśnięcie przycisku resetowania podczas wykonywania procedury może spowodować uszkodzenie woluminu i utratę danych.

Wszelkie operacje na woluminach dysków dynamicznych w systemach Windows XP i Windows 2000 można wykonywać tylko po uruchomieniu usługi Acronis Managed Machine Service na koncie z uprawnieniami administratora.

Aby uniknąć możliwej utraty danych, należy zastosować wszystkie niezbędne środki ostrożności (s. 265).

9.1 Obsługiwane systemy plików

Acronis Disk Director Lite obsługuje następujące systemy plików:

- FAT 16/32
- NTFS

Jeśli konieczne jest wykonanie operacji na woluminie z innym systemem plików, należy użyć pełnej wersji programu Acronis Disk Director. Oferuje ona więcej narzędzi umożliwiających zarządzanie dyskami i woluminami z następującymi systemami plików:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- partycja wymiany plików Linux SWAP

9.2 Podstawowe środki ostrożności

Aby uniknąć możliwego uszkodzenia struktury dysków i woluminów lub utraty danych, należy zastosować wszystkie niezbędne środki ostrożności oraz przestrzegać następujących prostych reguł:

1. Utwórz kopię zapasową dysku, na którym będzie się odbywało tworzenie woluminów lub zarządzanie nimi. Utworzenie kopii zapasowej najważniejszych danych na innym dysku twardym, w udziale sieciowym lub na nośniku wymiennym zagwarantuje bezpieczeństwo danych podczas pracy z woluminami dysku.
2. Sprawdź dysk, aby upewnić się, że jest w pełni sprawny i nie zawiera uszkodzonych sektorów ani błędów systemu plików.
3. Nie wykonuj żadnych operacji na dyskach/woluminach, gdy są uruchomione inne programy mające dostęp do dysków na niskim poziomie. Przed uruchomieniem narzędzia Acronis Disk Director Lite zamknij te programy.

Te proste środki ostrożności zapewniają ochronę przed przypadkową utratą danych.

9.3 Uruchamianie narzędzia Acronis Disk Director Lite

Narzędzie Acronis Disk Director Lite można uruchomić w systemie Windows lub z nośnika startowego.

Uruchamianie narzędzia Acronis Disk Director Lite w systemie Windows

Po uruchomieniu konsoli zarządzania Acronis Backup & Recovery 11 Management Console i podłączeniu jej do komputera zarządzanego, w drzewie **Nawigacja** konsoli będzie dostępny widok **Zarządzanie dyskami**, w którym można uruchomić narzędzie Acronis Disk Director Lite.

Uruchamianie narzędzia Acronis Disk Director Lite z nośnika startowego

Narzędzie Acronis Disk Director Lite można uruchomić w systemie odzyskanym po awarii, na komputerze, którego nie można uruchomić, albo na komputerze z systemem innym niż Windows. W tym celu należy uruchomić komputer z nośnika startowego (s. 381) utworzonego za pomocą generatora nośnika startowego Acronis, a następnie uruchomić konsolę zarządzania i kliknąć **Zarządzanie dyskami**.

9.4 Wybieranie systemu operacyjnego do zarządzania dyskami

Na komputerze, na którym znajdują się dwa lub więcej systemów operacyjnych, reprezentacja dysków i woluminów zależy od aktualnie uruchomionego systemu operacyjnego.

W różnych systemach operacyjnych Windows wolumin może mieć inną literę. Na przykład wolumin E: po uruchomieniu innego systemu operacyjnego Windows zainstalowanego na tym samym komputerze może być wyświetlany jako D: lub L:. (Jest także możliwe, że ten wolumin będzie miał tę samą literę E: w każdym systemie operacyjnym Windows zainstalowanym na komputerze).

Dysk dynamiczny utworzony w jednym systemie operacyjnym Windows może być uważany w innym systemie Windows za **dysk obcy** lub może w ogóle nie być obsługiwany przez ten system.

Aby wykonać na takim komputerze operację zarządzania dyskami, należy określić system operacyjny, dla którego będzie wyświetlany układ dysków i w którym będzie wykonywana operacja zarządzania dyskami.

Nazwa aktualnie wybranego systemu operacyjnego jest wyświetlana na pasku narzędzi konsoli za opcją „**Bieżący układ dysku**”. Aby wybrać inny system operacyjny w oknie **Wybór systemu operacyjnego**, należy kliknąć jego nazwę. Podczas pracy na nośniku startowym to okno pojawia się po kliknięciu **Zarządzanie dyskami**. Układ dysków będzie wyświetlany zgodnie z wybranym systemem operacyjnym.

9.5 Widok „Zarządzanie dyskami”

Do sterowania narzędziem Acronis Disk Director Lite służy widok **Zarządzanie dyskami** konsoli.

W górnej części widoku znajduje się tabela dysków i woluminów umożliwiającą sortowanie danych i dostosowywanie kolumn, a także pasek narzędzi. Tabela przedstawia numery dysków oraz przypisaną literę, etykietę, typ, pojemność, rozmiar wolnego miejsca, rozmiar używanego miejsca, system plików i status każdego woluminu. Pasek narzędzi składa się z ikon umożliwiających wykonywanie czynności **Cofnij**, **Wykonaj ponownie** i **Wykonaj** dotyczących operacji oczekujących (s. 280).

Panel graficzny w dolnej części widoku przedstawia graficzny obraz wszystkich dysków i ich woluminów w postaci prostokątów zawierających podstawowe dane na ich temat (etykieta, litera, rozmiar, status, typ i system plików).

Obie części widoku pokazują także całe nieprzydzielone miejsce na dysku, które można wykorzystać do tworzenia woluminów.

Uruchamianie operacji

Dowolną operację można uruchomić:

- z menu kontekstowego woluminu lub dysku (zarówno w tabeli, jak i w panelu graficznym),
- z menu **Zarządzanie dyskami** konsoli.
- z paska **Operacje** w panelu **Czynności i narzędzia**.

*Należy pamiętać, że lista operacji dostępnych w menu kontekstowym, w menu **Zarządzanie dyskami** i na pasku **Operacje** zależy od wybranego typu woluminu lub dysku. To samo dotyczy także nieprzydzielonego miejsca.*

Wyświetlanie wyników operacji

Wyniki dowolnej operacji na dysku lub woluminie, która została właśnie zaplanowana, są natychmiast wyświetlane w widoku **Zarządzanie dyskami** konsoli. Na przykład po utworzeniu woluminu zostanie on natychmiast wyświetlony w tabeli, a także w formie graficznej w dolnej części widoku. Również wszelkie zmiany woluminów, między innymi zmiana litery lub etykiety woluminu, są natychmiast wyświetlane w widoku.

9.6 Operacje na dyskach

Narzędzie Acronis Disk Director Lite umożliwia wykonywanie na dyskach następujących operacji:

- Inicjowanie dysku (s. 267) — inicjowanie nowego sprzętu dodanego do systemu
- Klonowanie dysku podstawowego (s. 267) — przenoszenie kompletnych danych ze źródłowego podstawowego dysku MBR na dysk docelowy
- Konwersja dysków: MBR na GPT (s. 270) — konwertowanie tabeli partycji MBR na GPT
- Konwersja dysków: GPT na MBR (s. 270) — konwertowanie tabeli partycji GPT na MBR

- Konwersja dysków: podstawowy na dynamiczny (s. 271) — konwertowanie dysku podstawowego na dynamiczny
- Konwersja dysków: dynamiczny na podstawowy (s. 272) — konwertowanie dysku dynamicznego na podstawowy

Pełna wersja programu Acronis Disk Director oferuje więcej narzędzi do pracy z dyskami.

Program Acronis Disk Director Lite musi uzyskać wyłączny dostęp do dysku docelowego. Oznacza to, że w tym czasie nie mogą z niego korzystać żadne inne narzędzia do zarządzania dyskami (na przykład narzędzie Windows Disk Management). Po wyświetleniu komunikatu informującego o tym, że nie można zablokować dysku, należy zamknąć aplikacje do zarządzania dyskami używające tego dysku i rozpocząć jeszcze raz. Jeśli nie można ustalić, które aplikacje używają dysku, należy zamknąć je wszystkie.

9.6.1 Inicjowanie dysku

Po dodaniu nowego dysku do komputera narzędzie Acronis Disk Director Lite wykryje zmianę konfiguracji i przeskanuje dodany dysk, aby uwzględnić go na liście dysków i woluminów. Jeśli dysk nie został zainicjowany lub system komputera nie rozpoznaje jego struktury plików, oznacza to, że na dysku tym nie można instalować programów ani przechowywać plików.

Narzędzie Acronis Disk Director Lite wykryje, że dysk nie może być używany przez system i wymaga zainicjowania. W widoku **Zarządzanie dyskami** nowo wykryty sprzęt będzie wyświetlany jako szary blok z wyszarzoną ikoną, co oznacza, że dysk nie może być używany w systemie.

Jeśli konieczna jest inicjalizacja dysku:

1. Wybierz dysk do inicjalizacji.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie w menu kontekstowym kliknij **Inicjuj**. Zostanie wyświetlone okno **Inicjowanie dysku**, w którym zostaną przedstawione podstawowe informacje o sprzęcie, takie jak numer, pojemność i stan dysku, które mogą pomóc w wybraniu odpowiedniej czynności.
3. Okno to umożliwia wybranie schematu partycjonowania dysku (MBR lub GPT) oraz typu dysku (podstawowy lub dynamiczny). Nowy stan dysku zostanie natychmiast przedstawiony w formie graficznej w widoku **Zarządzanie dyskami**.
4. Po kliknięciu przycisku **OK** zostanie dodana oczekująca operacja inicjacji dysku.

(Aby zakończyć dodawaną operację, należy ją przesłać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich anulowanie).

Po zakończeniu inicjowania całe miejsce na dysku jest nieprzydzielone, a więc nie może być używane do instalowania programów ani przechowywania plików. Aby umożliwić korzystanie z dysku, należy w normalny sposób wykonać operację **Utwórz wolumin**.

Jeśli zechcesz zmienić ustawienia dysku, możesz to zrobić później, używając standardowych funkcji dyskowych dostępnych w narzędziu Acronis Disk Director Lite.

9.6.2 Klonowanie dysku podstawowego

Czasami trzeba przenieść wszystkie dane z dysku na nowy dysk, na przykład podczas powiększania woluminu systemowego, uruchamiania nowego układu systemu lub ratowania dysku ze względu na usterkę sprzętową. W każdym z tych przypadków przyczynę operacji **Klonuj dysk podstawowy** można podsumować jako konieczność przeniesienia wszystkich danych z dysku źródłowego na dysk docelowy w dokładnie takiej samej postaci.

Narzędzie Acronis Disk Director Lite umożliwia wykonywanie tej operacji tylko na podstawowych dyskach MBR.

Aby zaplanować operację **Klonuj dysk podstawowy**:

1. Wybierz dysk do sklonowania.
2. Wybierz dysk docelowy operacji klonowania.
3. Wybierz metodę klonowania i określ opcje zaawansowane.

Nowa struktura woluminów zostanie natychmiast przedstawiona w formie graficznej w widoku **Zarządzanie dyskami**.

*Przed sklonowaniem dysku systemowego zaleca się wyłączenie funkcji Acronis Startup Recovery Manager (s. 375) (ASRM), jeśli jest aktywna. W przeciwnym razie sklonowany system operacyjny może się nie uruchamiać. Po zakończeniu klonowania można z powrotem włączyć funkcję ASRM. Jeśli dezaktywacja jest niemożliwa, należy wybrać metodę klonowania dysku **Tak jak jest**.*

Wybieranie dysku źródłowego i docelowego

Program wyświetla listę dysków podzielonych na partycje. Użytkownik musi wybrać dysk źródłowy, z którego dane zostaną przeniesione na inny dysk.

Kolejnym krokiem jest wybranie dysku docelowego operacji klonowania. Program umożliwia wybranie dysku, jeśli jego rozmiar wystarczy, aby pomieścić wszystkie dane z dysku źródłowego bez żadnych strat.

Jeśli na dysku wybranym jako docelowy znajdują się jakiekolwiek dane, zostanie wyświetlony komunikat: „**Wybrany dysk docelowy nie jest pusty. Dane w jego woluminach zostaną zastąpione.**”. Komunikat ten oznacza, że wszystkie dane, które aktualnie znajdują się na wybranym dysku docelowym, zostaną nieodwołalnie utracone.

Metoda klonowania i opcje zaawansowane

Operacja **Klonuj dysk podstawowy** zazwyczaj oznacza, że informacje z dysku źródłowego są przenoszone na dysk docelowy metodą „**Tak jak jest**”. Jeśli więc dysk docelowy ma taki sam rozmiar (lub jest większy), wszystkie informacje można na niego przenieść dokładnie w takiej postaci, w jakiej są przechowywane na dysku źródłowym.

Jednak w warunkach dużej różnorodności dostępnych urządzeń zazwyczaj dysk docelowy ma inny rozmiar niż dysk źródłowy. Jeśli dysk docelowy jest większy, warto wybrać opcję **Proporcjonalna zmiana rozmiaru woluminu**, która pozwala uniknąć pozostawienia na dysku docelowym nieprzydzielonego miejsca. Opcja **Klonuj dysk podstawowy** „tak jak jest” nie ulega zmianie, ale domyślna metoda klonowania jest wykonywana z proporcjonalnym powiększeniem wszystkich woluminów dysku **źródłowego**, aby na dysku **docelowym** nie pozostało nieprzydzielone miejsce.

Jeśli dysk docelowy jest mniejszy, opcja klonowania **Tak jak jest** jest niedostępna, natomiast konieczna staje się proporcjonalna zmiana rozmiaru woluminów dysku **źródłowego**. Program analizuje dysk **docelowy** w celu ustalenia, czy jego rozmiar wystarczy do pomieszczenia wszystkich danych z dysku **źródłowego** bez żadnych strat. Jeśli przeniesienie z proporcjonalną zmianą rozmiaru woluminów dysku **źródłowego** jest możliwe bez utraty danych, użytkownik może kontynuować. Jeśli ze względu na ograniczenia rozmiaru bezpieczne przeniesienie wszystkich danych z dysku **źródłowego** na dysk **docelowy** jest niemożliwe nawet w przypadku proporcjonalnej zmiany rozmiaru woluminów, wykonanie operacji **Klonuj dysk podstawowy** jest niemożliwe i użytkownik nie może kontynuować.

Jeśli klonowany ma być dysk zawierający **wolumin systemowy**, należy zwrócić uwagę na **Opcje zaawansowane**.

Kliknięcie **Zakończ** spowoduje dodanie oczekującej operacji klonowania dysku.

(Aby zakończyć dodawaną operację, należy ją wykonać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich anulowanie).

Używanie opcji zaawansowanych

W przypadku klonowania dysku zawierającego **wolumin systemowy** trzeba zachować możliwość uruchamiania systemu operacyjnego na woluminie dysku docelowego. Oznacza to, że w systemie operacyjnym informacje o woluminie systemowym (na przykład litera woluminu) muszą pasować do podpisu NT dysku, przechowywanego w jego rekordzie MBR. Ale dwa dyski o tym samym podpisie NT nie mogą działać prawidłowo w jednym systemie operacyjnym.

Jeśli dwa dyski w komputerze mają ten sam podpis NT i zawierają wolumin systemowy, podczas rozruchu system operacyjny uruchamia się z pierwszego dysku, wykrywa taki sam podpis na drugim dysku, automatycznie generuje nowy, unikatowy podpis NT i przypisuje go do drugiego dysku. Skutkiem tego wszystkie woluminy na drugim dysku tracą swoje litery, wszystkie ścieżki na dysku stają się nieprawidłowe, a programy nie mogą znaleźć swoich plików. Uruchomienie systemu operacyjnego umieszczonego na tym dysku jest niemożliwe.

Możliwość uruchamiania systemu na woluminie dysku docelowego można zachować przy użyciu jednej z dwóch opcji:

1. Kopiuj podpis NT — dysk docelowy otrzymuje podpis NT dysku źródłowego pasujący do kluczy rejestru także skopiowanych na dysk docelowy.
2. Pozostaw podpis NT — stary podpis dysku docelowego jest zachowywany, a system operacyjny jest aktualizowany odpowiednio do tego podpisu.

Jeśli trzeba skopiować podpis NT:

1. Zaznacz pole wyboru **Kopiuj podpis NT**. Zostanie wyświetlone ostrzeżenie: „Jeśli na dysku twardym znajduje się system operacyjny, przed ponownym uruchomieniem należy odinstalować źródłowy lub docelowy dysk twardy komputera. W przeciwnym razie system operacyjny zostanie uruchomiony z pierwszego z nich, a systemu operacyjnego znajdującego się na drugim dysku nie będzie można uruchomić”. Pole wyboru **Wyłącz komputer po wykonaniu operacji klonowania** jest zaznaczane i wyłączane automatycznie.
2. Kliknij **Zakończ**, aby dodać operację oczekującą.
3. Kliknij **Wykonaj** na pasku narzędzi, a następnie kliknij **Kontynuuj** w oknie **Operacje oczekujące**.
4. Zaczekaj na zakończenie operacji.
5. Zaczekaj na wyłączenie komputera.
6. Odłącz źródłowy lub docelowy dysk twardy od komputera.
7. Uruchom komputer.

Jeśli trzeba zachować podpis NT:

1. W razie potrzeby kliknij pole wyboru **Kopiuj podpis NT**, aby je wyczyścić.
2. W razie potrzeby kliknij pole wyboru **Wyłącz komputer po wykonaniu operacji klonowania**, aby je wyczyścić.
3. Kliknij **Zakończ**, aby dodać operację oczekującą.
4. Kliknij **Wykonaj** na pasku narzędzi, a następnie kliknij **Kontynuuj** w oknie **Operacje oczekujące**.
5. Zaczekaj na zakończenie operacji.

9.6.3 Konwersja dysków: MBR na GPT

Konwersja podstawowego dysku MBR na podstawowy dysk GPT może być konieczna w następujących przypadkach:

- Jeśli na jednym dysku potrzebnych jest więcej niż 4 woluminy podstawowe.
- Jeśli konieczna jest dodatkowa ochrona przed możliwym uszkodzeniem danych.

Jeśli konieczna jest konwersja podstawowego dysku MBR na podstawowy dysk GPT:

1. Wybierz podstawowy dysk MBR, który ma zostać przekonwertowany na dysk GPT.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Konwertuj na GPT** w menu kontekstowym.

Zostanie wyświetlone okno ostrzeżenia informujące o zamierzonym przekonwertowaniu dysku MBR na GPT.

3. Kliknięcie **OK** spowoduje dodanie operacji oczekującej konwersji dysku MBR na GPT.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Należy pamiętać, że dysk podzielony na partycje GPT rezerwuje na końcu obszaru partycji miejsce potrzebne na obszar kopii zapasowych, w którym są przechowywane kopie nagłówka GPT i tabeli partycji. Jeśli dysk jest pełny i nie można automatycznie zwiększyć rozmiaru woluminu, operacja konwersji dysku MBR na GPT zakończy się niepowodzeniem.

Operacja jest nieodwracalna. Jeśli wolumin podstawowy należący do dysku MBR zostanie przekonwertowany najpierw na dysk GPT, a następnie z powrotem na dysk MBR, stanie się woluminem logicznym i nie będzie można używać go jako woluminu systemowego.

Jeśli użytkownik planuje zainstalowanie systemu operacyjnego, który nie obsługuje dysków GPT, konwersja wsteczna na dysk MBR jest także możliwa za pośrednictwem tych samych elementów menu. Nazwa operacji będzie wyświetlana jako **Konwertuj na MBR**.

Konwersja dysków dynamicznych: MBR na GPT

Narzędzie Acronis Disk Director Lite nie obsługuje bezpośredniej konwersji dysków dynamicznych MBR na GPT. Jednak ten sam cel można osiągnąć przy użyciu programu, wykonując następujące konwersje:

1. Konwersja dysku MBR: dynamiczny na podstawowy (s. 272) przy użyciu operacji **Konwertuj na podstawowy**.
2. Konwersja dysku podstawowego: MBR na GPT przy użyciu operacji **Konwertuj na GPT**.
3. Konwersja dysku GPT: podstawowy na dynamiczny (s. 271) przy użyciu operacji **Konwertuj na dynamiczny**.

9.6.4 Konwersja dysku: GPT na MBR

Jeśli użytkownik planuje zainstalowanie systemu operacyjnego, który nie obsługuje dysków GPT, można przekonwertować dysk GPT na MBR. Nazwa operacji będzie wyświetlana jako **Konwertuj na MBR**.

Jeśli trzeba przekonwertować dysk GPT na MBR:

1. Wybierz dysk GPT, który ma zostać przekonwertowany na dysk MBR.

2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Konwertuj na MBR** w menu kontekstowym.

Zostanie wyświetlone okno ostrzeżenia informujące o zamierzonym przekonwertowaniu dysku GPT na MBR.

Zostaną wyświetlone informacje o zmianach, jakie dokonają się w systemie po przekonwertowaniu wybranego dysku GPT na MBR. Na przykład o tym, że jeśli tego rodzaju konwersja uniemożliwi dostęp systemu do dysku, po przeprowadzeniu konwersji system operacyjny przestanie się ładować lub niektóre woluminy z wybranego dysku GPT będą niedostępne na dysku MBR (np. woluminy znajdujące się w odległości większej niż 2 TB od początku dysku). Zostanie wyświetlone ostrzeżenie o tego rodzaju uszkodzeniach.

Należy pamiętać, że po wykonaniu tej operacji wolumin należący do konwertowanego dysku GPT stanie się woluminem logicznym i jest to nieodwracalne.

3. Kliknięcie **OK** powoduje dodanie operacji oczekującej konwersji dysku GPT na MBR.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

9.6.5 Konwersja dysku: podstawowy na dynamiczny

Konwersja dysku podstawowego na dynamiczny może być konieczna w następujących przypadkach:

- Dysk ma stanowić część grupy dysku dynamicznego.
- Chodzi o uzyskanie dodatkowej ochrony danych przechowywanych na dysku.

Jeśli trzeba przekonwertować dysk podstawowy na dynamiczny:

1. Wybierz dysk podstawowy, który ma zostać przekonwertowany na dynamiczny.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Konwertuj na dynamiczny** w menu kontekstowym. Zostanie wyświetlone ostatnie ostrzeżenie o konwersji dysku podstawowego na dynamiczny.
3. Kliknięcie **OK** w tym oknie ostrzeżenia spowoduje natychmiastowe wykonanie konwersji, a w razie potrzeby ponowne uruchomienie komputera.

Uwaga: dysk dynamiczny zajmuje ostatni megabajt dysku fizycznego w celu przechowywania bazy danych zawierającej czteropoziomowy opis każdego woluminu dynamicznego (Wolumin-Komponent-Partycja-Dysk). Jeśli podczas konwersji dysku na dynamiczny okaże się, że dysk podstawowy jest pełny i nie można automatycznie zmniejszyć rozmiaru jego woluminów, operacja konwersji dysku podstawowego na dynamiczny zakończy się niepowodzeniem.

Gdy użytkownik zdecyduje się na konwersję wsteczną dysków dynamicznych na podstawowe, na przykład w celu użycia systemu operacyjnego na komputerze, który nie obsługuje dysków dynamicznych, może przekonwertować dyski przy użyciu tych samych elementów menu, jednak tym razem operacja będzie nosiła nazwę **Konwertuj na podstawowy**.

Konwersja dysku systemowego

Narzędzie Acronis Disk Director Lite nie wymaga ponownego uruchomienia systemu operacyjnego po zakończeniu konwersji dysku podstawowego na dynamiczny, gdy:

1. na dysku jest zainstalowany jeden system operacyjny Windows 2008/Vista;
2. ten system operacyjny jest uruchomiony na komputerze.

Konwersja dysku podstawowego, składającego się z woluminów systemowych, na dysk dynamiczny zajmuje trochę czasu, a każda przerwa w dopływie zasilania, niezamierzone wyłączenie komputera lub przypadkowe

naciśnięcie przycisku Reset podczas wykonywania procedury może spowodować utratę możliwości uruchomienia.

W odróżnieniu od Menedżera dysków systemu Windows program zapewnia możliwość uruchomienia **systemu operacyjnego w trybie offline** na dysku po zakończeniu operacji.

9.6.6 Konwersja dysków: dynamiczne na podstawowe

Konwersja dysków dynamicznych na podstawowe może być konieczna na przykład w przypadku, gdy użytkownik chce rozpocząć korzystanie z systemu operacyjnego na komputerze, który nie obsługuje dysków dynamicznych.

Jeśli trzeba wykonać konwersję dysku dynamicznego na podstawowy:

1. Wybierz dysk dynamiczny, który ma zostać przekonwertowany na podstawowy.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Konwertuj na podstawowy** w menu kontekstowym. Zostanie wyświetlone ostatnie ostrzeżenie o konwersji dysku dynamicznego na podstawowy.

Zostaną wyświetlone informacje o zmianach, jakie dokonają się w systemie po przekonwertowaniu wybranego dysku dynamicznego na podstawowy, np. o tym, że jeśli tego rodzaju konwersja uniemożliwi dostęp systemu do dysku, po przeprowadzeniu konwersji system operacyjny przestanie się ładować. Jeśli natomiast dysk przeznaczony do konwersji na podstawowy zawiera jakiegokolwiek woluminy, których typy są obsługiwane wyłącznie przez dyski dynamiczne (wszystkie typy woluminów, z wyjątkiem woluminów prostych), w tym miejscu zostanie wyświetlone ostrzeżenie o możliwości uszkodzenia konwertowanych danych.

Należy pamiętać, że operacja jest niedostępna w przypadku dysku dynamicznego zawierającego woluminy łączone, rozłożone lub RAID-5.

3. Kliknięcie **OK** w tym oknie ostrzeżenia spowoduje natychmiastowe wykonanie konwersji.

Po zakończeniu konwersji ostatnie 8 MB miejsca na dysku jest rezerwowane na potrzeby konwersji dysku z podstawowego na dynamiczny w przyszłości.

W niektórych przypadkach możliwe nieprzydzielone miejsce i proponowany maksymalny rozmiar woluminu mogą się różnić (np. gdy rozmiar jednego woluminu lustrzanego ustala rozmiar drugiego lub gdy ostatnie 8 MB miejsca na dysku zostaje zarezerwowane na potrzeby konwersji dysku z podstawowego na dynamiczny w przyszłości).

Konwersja dysku systemowego

w następujących przypadkach narzędzie Acronis Disk Director Lite nie wymaga ponownego uruchomienia systemu operacyjnego po zakończeniu konwersji dysku dynamicznego na podstawowy:

1. Na dysku jest zainstalowany jeden system operacyjny Windows 2008/Vista.
2. Ten system operacyjny jest uruchomiony na komputerze.

Konwersja dysku dynamicznego, składającego się z woluminów systemowych, na dysk podstawowy zajmuje trochę czasu, a każda przerwa w dopływie zasilania, niezamierzone wyłączenie komputera lub przypadkowe naciśnięcie przycisku Reset podczas wykonywania procedury może spowodować utratę możliwości uruchomienia.

W odróżnieniu od Menedżera dysków systemu Windows program zapewnia:

- bezpieczną konwersję dysku dynamicznego na podstawowy, gdy zawiera on woluminy **z danymi** woluminów prostych i lustrzanych;

- na komputerach z funkcją uruchamiania wielu systemów operacyjnych możliwość uruchomienia systemu, który w czasie operacji znajdował się w trybie **offline**.

9.6.7 Zmiana statusu dysku

Zmiana statusu dysku, możliwa w systemach operacyjnych Windows Vista SP1, Windows Server 2008 i Windows 7, ma zastosowanie do bieżącego układu dysku (s. 265).

W widoku graficznym dysku obok jego nazwy zawsze wyświetlany jest jeden z następujących statusów dysku:

- **Online**
Status online oznacza, że dysk jest dostępny w trybie do odczytu i zapisu. Jest to normalny status dysku. Jeśli dysk ma być dostępny w trybie tylko do odczytu, wybierz dysk i zmień jego status na offline, wybierając **Zmień status dysku na offline** z menu **Operacje**.
- **Offline**
Status offline oznacza, że dysk jest dostępny w trybie tylko do odczytu. Aby z powrotem ustawić status online dysku, wybierz **Zmień status dysku na online** z menu **Operacje**.
Jeśli dysk ma status offline i nazwę **Brakujący**, oznacza to, że system operacyjny nie może znaleźć lub rozpoznać dysku. Dysk może być uszkodzony, odłączony lub wyłączony. Aby uzyskać informacje o przywracaniu brakującego dysku o statusie offline do statusu online, zobacz następujący artykuł z bazy wiedzy firmy Microsoft: <http://technet.microsoft.com/en-us/library/cc732026.aspx>.

9.7 Operacje w woluminach

Narzędzie Acronis Disk Director Lite umożliwia wykonywanie następujących operacji na woluminach:

- Utwórz wolumin (s. 273) — tworzy nowy wolumin z pomocą Kreatora tworzenia woluminów.
- Usuń wolumin (s. 277) — usuwa wybrany wolumin.
- Set Active (s. 278) (Ustaw jako aktywny) — ustawia wybrany wolumin jako aktywny, aby umożliwić uruchamianie komputera z zainstalowanym w tym woluminie systemem operacyjnym.
- Zmień literę (s. 278) — zmienia literę wybranego woluminu.
- Zmień etykietę (s. 279) — zmienia etykietę wybranego woluminu.
- Formatowanie woluminu (s. 279) — formatuje wolumin, zapewniając mu niezbędny system plików.

Pełna wersja programu Acronis Disk Director oferuje więcej narzędzi do pracy z woluminami.

Program Acronis Disk Director Lite musi uzyskać wyłączny dostęp do woluminu docelowego. Oznacza to, że w tym czasie nie mogą z niego korzystać żadne inne narzędzia do zarządzania dyskami (na przykład narzędzie Windows Disk Management). Po wyświetleniu komunikatu informującego o tym, że nie można zablokować woluminu, należy zamknąć aplikacje do zarządzania dyskami używające tego woluminu i rozpocząć jeszcze raz. Jeśli nie można ustalić, które aplikacje używają woluminu, należy zamknąć je wszystkie.

9.7.1 Tworzenie woluminu

Nowy wolumin może być potrzebny do:

- odzyskania zapisanej wcześniej kopii zapasowej w konfiguracji „dokładnie tak, jak był”;

- oddzielnego przechowywania kolekcji podobnych plików, na przykład kolekcji MP3 lub plików wideo w oddzielnym woluminie;
- przechowywania kopii zapasowych (obrazów) innych woluminów/dysków w woluminie specjalnym;
- zainstalowania nowego systemu operacyjnego (lub pliku wymiany) w nowym woluminie;
- dodania nowego sprzętu do komputera.

W programie Acronis Disk Director Lite do tworzenia woluminów służy **Kreator tworzenia woluminów**.

Typy woluminów dynamicznych

Wolumin prosty

Wolumin utworzony z wolnego miejsca na pojedynczym dysku fizycznym. Może składać się z jednego regionu na dysku lub z kilku regionów połączonych wirtualnie przez Menedżera dysków logicznych (LDM). Nie zapewnia większej niezawodności, większej szybkości ani dodatkowego miejsca.

Wolumin łączony

Wolumin utworzony z wolnego miejsca na kilku dyskach fizycznych, połączony wirtualnie przez LDM. Jeden wolumin może obejmować maksymalnie 32 dyski, co pozwala na pokonanie sprzętowych ograniczeń rozmiaru, ale awaria jednego dysku spowoduje utratę wszystkich danych. Nie można również usunąć żadnej części woluminu łączonego, nie niszcząc całego woluminu. Dlatego wolumin łączony nie zapewnia większej niezawodności ani większej szybkości wykonywania operacji wejścia/wyjścia.

Wolumin rozłożony

Wolumin (nazywany czasami RAID 0) składający się z równych fragmentów danych rozłożonych między poszczególne dyski w woluminie. Oznacza to, że do utworzenia woluminu rozłożonego użytkownik potrzebuje dwóch lub więcej dysków dynamicznych. Dyski w woluminie rozłożonym nie muszą być identyczne, ale na każdym dysku, który ma zostać uwzględniony w woluminie, musi być dostępne nieużywane miejsce, a rozmiar woluminu będzie zależał od rozmiaru najmniejszego miejsca. Dostęp do danych w woluminie rozłożonym jest zazwyczaj szybszy niż do tych samych danych na pojedynczym dysku fizycznym, ponieważ operacje wejścia/wyjścia są rozłożone na kilka dysków.

Woluminy rozłożone tworzy się w celu zwiększenia wydajności, a nie ze względu na większą niezawodność — nie zawierają one nadmiarowych informacji.

Wolumin lustrzany

Wolumin odporny na uszkodzenia (nazywany czasami RAID 1), którego dane są zduplikowane na dwóch identycznych dyskach fizycznych. Wszystkie dane z jednego dysku są kopiowane na drugi dysk w celu zapewnienia nadmiarowości danych. Woluminem lustrzanym może być prawie każdy wolumin, w tym również systemowy i startowy. Jeśli jeden dysk ulegnie uszkodzeniu, dane wciąż będą dostępne na pozostałych dyskach. Niestety, w przypadku korzystania z woluminów lustrzanych sprzętowe ograniczenia rozmiaru i wydajności są jeszcze większe.

Wolumin lustrzany-rozłożony

Wolumin odporny na uszkodzenia (nazywany czasami RAID 1+0), łączący w sobie zalety dużej szybkości operacji wejścia/wyjścia w układzie rozłożonym z nadmiarowością, jaką zapewnia typ lustrzany. Oczwistą wadą wynikającą z architektury lustrzanej jest niski współczynnik rozmiaru dysku do rozmiaru woluminu.

RAID-5

Wolumin odporny na uszkodzenia, którego dane rozkładają się na trzy lub więcej dysków. Dyski nie muszą być identyczne, ale na każdym dysku w woluminie muszą być dostępne równej wielkości bloki nieprzydzielonego miejsca. Także parzystość (obliczona wartość, która może zostać użyta do rekonstrukcji danych w przypadku uszkodzenia) jest rozłożona na całej macierzy dyskowej. Ponadto jest ona zawsze przechowywana na innym dysku niż same dane. W przypadku awarii dysku fizycznego część woluminu RAID-5 znajdująca się na uszkodzonym dysku może zostać odtworzona na podstawie pozostałych danych i parzystości. Wolumin RAID-5 zapewnia niezawodność i umożliwia przekroczenie ograniczeń związanych z rozmiarem dysku fizycznego dzięki wyższemu wskaźnikowi dysku lustrzany/rozmiar woluminu.

Kreator tworzenia woluminów

Kreator tworzenia woluminów pozwala na utworzenie dowolnego typu woluminu (w tym również systemowego i aktywnego), wybranie systemu plików, opatrzenie etykietą, przypisanie litery. Zawiera także inne funkcje zarządzania dyskami.

Na jego stronach można wprowadzać parametry operacji, wykonywać kolejne operacje, a w razie potrzeby wracać do poprzednich czynności w celu zmiany dowolnych wybranych wcześniej opcji. W dokonaniu wyboru pomagają szczegółowe instrukcje dotyczące poszczególnych parametrów.

Aby utworzyć wolumin:

Należy uruchomić **Kreator tworzenia woluminów**, wybierając **Utwórz wolumin** na pasku **Kreatory**, lub kliknąć prawym przyciskiem myszy dowolne nieprzydzielone miejsce i wybrać **Utwórz wolumin** w wyświetlonym menu kontekstowym.

Wybierz typ tworzonego woluminu

Najpierw należy określić typ woluminu, który ma zostać utworzony. Dostępne są następujące typy woluminów:

- Podstawowy
- Prosty/łączony
- Rozłożony
- Lustrzany
- RAID-5

Każda możliwa architektura woluminów zostanie opatrzona krótkim opisem, co umożliwia lepsze zrozumienie jej zalet i ograniczeń.

*Jeśli bieżący system operacyjny zainstalowany na tym komputerze nie obsługuje wybranego typu woluminu, zostanie wyświetlone odpowiednie ostrzeżenie. W takim przypadku przycisk **Dalej** będzie wyłączony i trzeba będzie wybrać inny typ woluminu, aby kontynuować tworzenie nowego woluminu.*

Po kliknięciu przycisku **Dalej** nastąpi przejście do strony kreatora: Wybierz dyski docelowe (s. 275).

Wybierz dyski docelowe

Na następnej stronie kreatora zostanie wyświetlony monit o wybranie dysków z miejscem do tworzenia woluminu.

Aby utworzyć wolumin podstawowy:

- Wybierz dysk docelowy i określ nieprzydzielone miejsce, aby utworzyć w nim wolumin podstawowy.

Aby utworzyć wolumin prosty/łączony:

- Wybierz jeden lub więcej dysków docelowych, aby utworzyć na nich wolumin.

Aby utworzyć wolumin lustrzany:

- Wybierz dwa dyski docelowe, na których zostanie utworzony wolumin.

Aby utworzyć wolumin rozłożony:

- Wybierz dwa lub więcej dysków docelowych, aby utworzyć na nich wolumin.

Aby utworzyć wolumin RAID-5:

- Wybierz trzy dyski docelowe, na których zostanie utworzony wolumin.

Po wybraniu dysków kreator obliczy maksymalny rozmiar woluminu wynikowego w zależności od rozmiaru nieprzydzielonego miejsca na wybranych dyskach oraz wymagań wybranego wcześniej typu woluminu.

Jeśli użytkownik tworzy wolumin **dynamiczny** i jako miejsce docelowe wybierze jeden lub kilka dysków **podstawowych**, zostanie wyświetlone ostrzeżenie, że wybrany dysk zostanie automatycznie przekonwertowany na dynamiczny.

W razie potrzeby zostanie wyświetlony monit o dodanie niezbędnej liczby dysków, zgodnie z wybranym typem przyszłego woluminu.

Kliknięcie przycisku **Wstecz** spowoduje powrót do strony: Wybierz typ tworzonego woluminu (s. 275).

Kliknięcie przycisku **Dalej** spowoduje przejście do strony: Ustaw rozmiar woluminu (s. 276).

Ustaw rozmiar woluminu

Na trzeciej stronie kreatora można określić rozmiar przyszłego woluminu, zgodnie z wybranymi wcześniej opcjami. W celu wybrania niezbędnego rozmiaru z zakresu od wartości minimalnej do wartości maksymalnej należy użyć suwaka, wprowadzić potrzebne wartości w specjalnych oknach lub kliknąć specjalny uchwyt, a następnie przytrzymać i przeciągnąć granice obrazu dysku za pomocą kursora.

Wartość maksymalna zazwyczaj obejmuje największe możliwe nieprzydzielone miejsce. Jednak w niektórych przypadkach możliwe nieprzydzielone miejsce i proponowany maksymalny rozmiar woluminu mogą się różnić (np. gdy rozmiar jednego woluminu lustrzanego ustala rozmiar drugiego lub gdy 8 MB miejsca na dysku zostaje zarezerwowane na potrzeby konwersji dysku z podstawowego na dynamiczny w przyszłości).

W przypadku woluminów podstawowych pozostawienie na dysku pewnej ilości nieprzydzielonego miejsca umożliwi także wybranie położenia nowego woluminu na dysku.

Kliknięcie przycisku **Wstecz** spowoduje powrót do strony: Wybierz dyski docelowe (s. 275).

Kliknięcie przycisku **Dalej** spowoduje przejście do strony: Ustaw opcje woluminu (s. 277).

Ustaw opcje woluminu

Na następnej stronie kreatora można przypisać **literę** woluminu (domyślnie jest to pierwsza wolna litera alfabetu) oraz opcjonalnie jego **etykietę** (domyślnie brak). W tym miejscu można także określić **system plików** i **rozmiar klastra**.

Kreator wyświetli monit o wybranie jednego z systemów plików systemu Windows: FAT16 (wyłączony, gdy ustawiono rozmiar woluminu większy niż 2 GB), FAT32 (wyłączony, gdy ustawiono rozmiar woluminu większy niż 32 GB) lub NTFS. Można także zostawić wolumin **niesformatowany**.

Ustawiając rozmiar klastra, można wybrać dowolną liczbę spośród wstępnie ustawionych wartości dla każdego systemu plików. Należy pamiętać, że program proponuje rozmiar klastra najlepiej dopasowany do woluminu z wybranym systemem plików.

Jeśli użytkownik tworzy wolumin podstawowy, który może być woluminem systemowym, ta strona wygląda inaczej, ponieważ umożliwia wybranie **typu** woluminu — **podstawowego (aktywnego podstawowego)** lub **logicznego**.

Zazwyczaj typ **Podstawowy** wybiera się, aby zainstalować w woluminie system operacyjny. Wartość **Aktywny** (domyślnie) należy wybrać, aby zainstalować w tym woluminie system operacyjny, który będzie uruchamiany podczas rozruchu komputera. Jeśli nie zostanie wybrany przycisk **Podstawowy**, opcja **Aktywny** będzie wyłączona. Jeśli wolumin ma służyć do magazynowania danych, należy wybrać opcję **Logiczny**.

*Dysk podstawowy może zawierać maksymalnie cztery woluminy podstawowe. Jeśli woluminy już istnieją, dysk trzeba przekonwertować na dynamiczny, w przeciwnym razie opcje **Aktywny** i **Podstawowy** będą wyłączone i będzie można wybrać wyłącznie typ woluminu **Logiczny**. Komunikat ostrzegawczy poinformuje, że nie będzie można uruchomić systemu operacyjnego zainstalowanego w tym woluminie.*

*Jeśli do ustawiania etykiety nowego woluminu będą używane znaki, które nie są obsługiwane przez aktualnie zainstalowany system operacyjny, zostanie wyświetlone odpowiednie ostrzeżenie, a przycisk **Dalej** będzie wyłączony. Aby kontynuować tworzenie nowego woluminu, należy zmienić etykietę.*

Kliknięcie przycisku **Wstecz** spowoduje powrót do strony: Ustaw rozmiar woluminu (s. 276).

Kliknięcie przycisku **Zakończ** spowoduje zakończenie planowania operacji.

Aby wykonać zaplanowaną operację, należy kliknąć **Wykonaj** na pasku narzędzi, a następnie kliknąć **Kontynuuj** w oknie **Operacje oczekujące**.

W przypadku ustawienia rozmiaru klastra 64 KB w systemie FAT16/FAT32 lub 8 KB–64 KB w systemie NTFS system Windows będzie mógł zamontować wolumin, ale niektóre programy (np. programy instalacyjne) mogą niepoprawnie obliczać miejsce na dysku.

9.7.2 Usuń wolumin

Ta wersja programu Acronis Disk Director Lite ma ograniczoną funkcjonalność, ponieważ głównym zadaniem tego narzędzia jest przygotowywanie systemów odzyskanych po awarii do odzyskiwania zapisanych wcześniej obrazów woluminów. Funkcje zmiany rozmiaru istniejących woluminów i tworzenia nowych woluminów przy użyciu wolnego miejsca w istniejących woluminach są dostępne w pełnej wersji oprogramowania, dlatego w tej wersji usunięcie istniejącego woluminu czasami może być jedynym sposobem zwolnienia potrzebnego miejsca na dysku bez zmiany istniejącej konfiguracji dysków.

Po usunięciu woluminu jego miejsce jest dodawane do nieprzydzielonego miejsca na dysku. Można go użyć do utworzenia nowego woluminu lub do zmiany typu innego woluminu.

Aby usunąć wolumin:

1. Wybierz dysk twardy i wolumin do usunięcia.
2. Wybierz **Usuń wolumin** lub podobny element na liście paska bocznego **Operacje** bądź kliknij ikonę **Usuń wybrany wolumin** na pasku narzędzi.

Jeśli wolumin zawiera jakiekolwiek dane, zostanie wyświetlone ostrzeżenie, że wszystkie informacje w tym woluminie zostaną nieodwracalnie utracone.

3. Kliknięcie **OK** w oknie **Usuń wolumin** powoduje dodanie operacji oczekującej usuwania woluminu.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

9.7.3 Ustaw aktywny wolumin

Jeśli istnieje kilka woluminów podstawowych, należy określić jeden, który będzie woluminem startowym. W tym celu można ustawić wolumin, który stanie się woluminem aktywnym. Na dysku może znajdować się tylko jeden wolumin aktywny, dlatego jeśli wolumin zostanie ustawiony jako aktywny, wolumin, który był aktywny poprzednio, automatycznie przestanie być woluminem aktywnym.

Jeśli trzeba ustawić wolumin jako aktywny:

1. Wybierz wolumin podstawowy na podstawowym dysku MBR, aby ustawić go jako aktywny.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Oznacz jako aktywną** w menu kontekstowym.

Jeśli w systemie nie ma żadnego innego woluminu aktywnego, zostanie dodana operacja oczekująca ustawiania woluminu aktywnego.

Należy pamiętać, że w wyniku ustawienia nowego woluminu aktywnego może się zmienić litera poprzedniego woluminu aktywnego, co przez co uruchamianie niektórych zainstalowanych programów może być niemożliwe.

3. Jeśli w systemie znajduje się inny wolumin aktywny, najpierw zostanie wyświetlone ostrzeżenie, że poprzedni wolumin aktywny został ustawiony jako pasywny. Kliknięcie **OK** w oknie **Ostrzeżenie** powoduje dodanie operacji oczekującej ustawiania woluminu aktywnego.

Należy pamiętać, że nawet jeśli w nowym woluminie aktywnym znajduje się system operacyjny, w niektórych przypadkach nie można uruchomić komputera za jego pomocą. Decyzję o ustawieniu nowego woluminu jako aktywnego trzeba potwierdzić.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Nowa struktura woluminów zostanie natychmiast przedstawiona w formie graficznej w widoku **Zarządzanie dyskami**.

9.7.4 Zmień literę woluminu

Systemy operacyjne Windows przypisują litery (C:, D: itd.) do woluminów dysku twardego przy uruchamianiu. Litery te są używane przez aplikacje i systemy operacyjne do znajdowania plików i folderów w woluminach.

Podłączenie dodatkowego dysku oraz utworzenie lub usunięcie woluminu na istniejących dyskach może spowodować zmianę konfiguracji systemu. W rezultacie niektóre aplikacje mogą przestać działać prawidłowo. Także automatyczne znajdowanie i otwieranie plików użytkownika może okazać się niemożliwe. Aby temu zapobiec, można ręcznie zmienić litery, które zostały automatycznie przypisane do woluminów przez system operacyjny.

Jeśli trzeba zmienić literę przypisaną do woluminu przez system operacyjny:

1. Wybierz wolumin do zmiany litery.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Zmień literę** w menu kontekstowym.
3. Wybierz nową literę w oknie **Zmień literę**.
4. Kliknięcie **OK** w oknie **Zmień literę** powoduje dodanie operacji oczekującej przypisywania litery woluminu.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Nowa struktura woluminów zostanie natychmiast przedstawiona w formie graficznej w widoku **Zarządzanie dyskami**.

9.7.5 Zmień etykietę woluminu

Etykieta woluminu to atrybut opcjonalny. Jest to nazwa przypisana do woluminu, która ułatwia jego rozpoznawanie. Na przykład wolumin może mieć nazwę SYSTEM (wolumin z systemem operacyjnym), PROGRAM (wolumin aplikacji), DANE (wolumin danych) itp., ale to nie oznacza, że w takim woluminie można magazynować wyłącznie dane typu podanego na etykiecie.

W systemie Windows etykiety woluminów są pokazywane w drzewie dysków i folderów Eksploratora: WIN98(C:), WINXP(D:), DANE(E:) itp. WIN98, WINXP i DANE to etykiety woluminów. Etykieta woluminu jest pokazywana we wszystkich oknach dialogowych aplikacji umożliwiających otwieranie i zapisywanie plików.

Jeśli trzeba zmienić etykietę woluminu:

1. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Zmień etykietę**.
2. Wprowadź nową etykietę w polu tekstowym okna **Zmień etykietę**.
3. Kliknięcie **OK** w oknie **Zmień etykietę** powoduje dodanie operacji oczekującej zmiany etykiety woluminu.

*Jeśli do ustawiania etykiety nowego woluminu będą używane znaki, które nie są obsługiwane przez aktualnie zainstalowany system operacyjny, zostanie wyświetlone odpowiednie ostrzeżenie, a przycisk **OK** będzie wyłączony. Aby kontynuować zmienianie etykiety woluminu, należy używać wyłącznie obsługiwanych znaków.*

(Aby zakończyć dodaną operację, należy ją wykonać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Nowa etykieta zostanie natychmiast przedstawiona w formie graficznej w widoku **Zarządzanie dyskami** konsoli.

9.7.6 Formatowanie woluminu

Wolumin można sformatować, aby zmienić jego system plików:

- w celu zaoszczędzenia dodatkowego miejsca, które jest tracone z powodu rozmiaru klastra w systemach plików FAT16 i FAT32;
- w celu szybkiego i dość skutecznego zniszczenia danych znajdujących się w tym woluminie.

Aby sformatować wolumin:

1. Wybierz wolumin do sformatowania.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Formatuj** w menu kontekstowym.

Zostanie otwarte okno **Formatowanie woluminu**, w którym można ustawić opcje nowego systemu plików. Do wyboru jest jeden z systemów plików systemu Windows: FAT16 (wyłączony, gdy rozmiar woluminu jest większy niż 2 GB), FAT32 (wyłączony, gdy rozmiar woluminu jest większy niż 32 GB) lub NTFS.

W razie potrzeby w oknie tekstowym można wprowadzić etykietę woluminu. Domyślnie to okno jest puste.

Ustawiając rozmiar klastra, można wybrać dowolną liczbę spośród wstępnie ustawionych wartości dla każdego systemu plików. Należy pamiętać, że program proponuje rozmiar klastra najlepiej dopasowany do woluminu z wybranym systemem plików.

3. Kliknięcie **OK** w celu kontynuowania operacji **Formatowanie woluminu** powoduje dodanie operacji oczekującej formatowania woluminu.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 280). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Nowa struktura woluminów zostanie przedstawiona w formie graficznej w widoku **Zarządzanie dyskami**.

W przypadku ustawienia rozmiaru klastra 64 KB w systemie FAT16/FAT32 lub 8 KB–64 KB w systemie NTFS system Windows będzie mógł zamontować wolumin, ale niektóre programy (np. programy instalacyjne) mogą niepoprawnie obliczać miejsce na dysku.

9.8 Operacje oczekujące

Wszystkie operacje, które zostały przygotowane przez użytkownika w trybie ręcznym lub za pomocą kreatora, są uważane za oczekujące, dopóki użytkownik nie wyda określonego polecenia powodującego trwałe wprowadzenie zmian. Do tego czasu narzędzie Acronis Disk Director Lite prezentuje jedynie nową strukturę woluminów, która powstanie w wyniku wykonania operacji zaplanowanych na dyskach i woluminach. Ta metoda umożliwia kontrolę wszystkich zaplanowanych operacji, ponowne sprawdzenie zamierzonych zmian, a w razie potrzeby anulowanie operacji przed ich wykonaniem.

Aby zapobiec wprowadzeniu jakiegokolwiek niezamierzonej zmiany na dysku, program najpierw wyświetli listę wszystkich operacji oczekujących.

W widoku **Zarządzanie dyskami** znajduje się pasek narzędzi z ikonami umożliwiającymi wykonywanie czynności **Cofnij**, **Wykonaj ponownie** i **Wykonaj** dotyczących operacji oczekujących. Czynności te można także wykonywać z menu **Zarządzanie dyskami** konsoli.

Wszystkie zaplanowane operacje są dodawane do listy operacji oczekujących.

Czynność **Cofnij** umożliwia cofnięcie ostatniej operacji na liście. Ta czynność jest dostępna, dopóki lista nie jest pusta.

Czynność **Wykonaj ponownie** umożliwia przywrócenie ostatniej operacji oczekującej, która została cofnięta.

Czynność **Wykonaj** powoduje otwarcie okna **Operacje oczekujące**, w którym można wyświetlić listę tych operacji. Kliknięcie **Kontynuuj** spowoduje ich wykonanie. Po wybraniu operacji **Kontynuuj** nie można cofnąć żadnych czynności ani operacji. Klikając **Anuluj**, można także anulować zamiar wykonania operacji. Dzięki temu na liście operacji oczekujących nie zostaną wprowadzone żadne zmiany.

Zamknięcie narzędzia Acronis Disk Director Lite bez wykonania operacji oczekujących oznacza ich skuteczne anulowanie, dlatego próba zamknięcia widoku **Zarządzanie dyskami** bez wykonania operacji oczekujących powoduje wyświetlenie odpowiedniego ostrzeżenia.

10 Administrowanie komputerem zarządzanym

W tej sekcji opisano widoki dostępne za pośrednictwem drzewa nawigacji w konsoli podłączonej do komputera zarządzanego oraz omówiono sposoby pracy w każdym widoku.

10.1 Plany i zadania tworzenia kopii zapasowych

Widok **Plany i zadania tworzenia kopii zapasowych** zawiera informacje o poziomie zabezpieczeń danych na określonym komputerze. Umożliwia on monitorowanie planów i zadań tworzenia kopii zapasowych oraz zarządzanie nimi.

Aby dowiedzieć się, jakie działania na komputerze wykonuje w danym momencie plan tworzenia kopii zapasowych, należy sprawdzić stan wykonania planu (s. 285). Stan wykonywania planu tworzenia kopii zapasowych to łączny stan ostatnich działań tego planu. Status planu tworzenia kopii zapasowych (s. 285) ułatwia określenie, czy dane są skutecznie chronione.

W celu śledzenia bieżącego postępu zadania należy sprawdzać jego stan (s. 286). Sprawdzając status (s. 286) zadania, można ustalić jego wynik.

Typowy przepływ roboczy

- Aby w tabeli planów tworzenia kopii zapasowych wyświetlić żądane plany (zadania), skorzystaj z filtrów. Domyślnie w tabeli są wyświetlane wszystkie plany z komputera zarządzanego posortowane według nazwy. Możesz również ukrywać niepotrzebne kolumny i wyświetlać kolumny ukryte. Aby uzyskać szczegółowe informacje, zobacz „Sortowanie, filtrowanie i konfigurowanie elementów tabeli” (s. 26).
- W tabeli kopii zapasowych należy wybrać plan (zadanie) tworzenia kopii zapasowych.
- Aby wykonać czynność dotyczącą wybranego planu (zadania), użyj przycisków na pasku narzędzi. Aby uzyskać szczegółowe informacje, zobacz „Czynności dotyczące planów i zadań tworzenia kopii zapasowych” (s. 282).
- Aby przejrzeć szczegółowe informacje na temat wybranego planu (zadania), skorzystaj z panelu informacyjnego w dolnej części okna. Panel jest domyślnie zwinięty. Aby go rozwinąć, kliknij symbol strzałki (▲). Zawartość panelu jest także dostępna odpowiednio w oknach **Szczegóły planu** (s. 292) i **Szczegóły zadania** (s. 293).







10.1.1 Czynności dotyczące planów i zadań tworzenia kopii zapasowych

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na planach i zadaniach tworzenia kopii zapasowych.

Ograniczenia

- Jeśli użytkownik nie ma na komputerze uprawnień administratora, nie może uruchamiać ani modyfikować planów ani zadań należących do innych użytkowników.
- Nie jest możliwa modyfikacja ani usunięcie aktualnie uruchomionego planu ani zadania tworzenia kopii zapasowych.

- Scentralizowany plan lub zadanie tworzenia kopii zapasowych może być zmodyfikowane lub usunięte tylko po stronie serwera zarządzania.

Zadanie	Czynności
Utworzenie nowego planu lub zadania tworzenia kopii zapasowych	<p>Kliknij  Nowy i wybierz jedną z następujących opcji:</p> <ul style="list-style-type: none"> ▪ Plan tworzenia kopii zapasowych (s. 48) ▪ Zadanie odzyskiwania (s. 130) ▪ Zadanie sprawdzania poprawności (s. 231)
Wyświetlanie szczegółów planu lub zadania	<p>Kliknij  Szczegóły.</p> <p>W odpowiednim oknie Szczegóły planu (s. 292) lub Szczegóły zadania (s. 293) przejrzyj szczegółowe informacje na temat planu lub zadania.</p>
Wyświetlanie dziennika planu lub zadania	<p>Kliknij  Dziennik.</p> <p>Nastąpi przejście do widoku Dziennik (s. 293) zawierającego listę wpisów dziennika pogrupowanych według działań związanych z planem/zadaniem.</p>
Uruchamianie planu lub zadania	<p><u>Plan tworzenia kopii zapasowych</u></p> <ol style="list-style-type: none"> 1. Kliknij  Uruchom. 2. Z listy rozwijanej wybierz w ramach planu zadanie, które należy uruchomić. <p>Uruchomienie planu tworzenia kopii zapasowych powoduje natychmiastowe uruchomienie wybranego zadania, niezależnie od jego harmonogramu i warunków.</p> <p><u>Zadanie</u></p> <p>Kliknij  Uruchom.</p> <p>Zadanie zostanie wykonane natychmiast, niezależnie od harmonogramu i warunków.</p>
Zatrzymywanie planu lub zadania	<p>Kliknij  Zatrzymaj.</p> <p><u>Plan tworzenia kopii zapasowych</u></p> <p>Zatrzymanie wykonywanego planu tworzenia kopii zapasowej powoduje zatrzymanie wszystkich jego zadań. Dlatego wszystkie operacje zadań zostaną przerwane.</p> <p><u>Zadanie</u></p> <p>Zatrzymanie zadania spowoduje przerwanie jego operacji (odzyskiwania, sprawdzania poprawności, eksportowania, konwersji itp.) Zadanie przejdzie w stan Bezczynne. Ewentualny harmonogram zadania pozostanie ważny. Aby dokończyć operację, trzeba będzie uruchomić zadanie od początku.</p> <p>Co się stanie, jeśli zatrzymam zadanie odzyskiwania?</p> <ul style="list-style-type: none"> ▪ Odzyskiwanie dysków: przerwana operacja może spowodować zmiany na dysku docelowym. W zależności od czasu, jaki upłynął od momentu uruchomienia zadania, dysk docelowy może nie być zainicjowany, miejsce na dysku może być nieprzydzielone lub niektóre woluminy mogą być odzyskane, a inne nie. Aby odzyskać cały dysk, należy ponownie uruchomić zadanie. ▪ Odzyskiwanie woluminów: wolumin docelowy zostanie usunięty, a jego miejsce stanie się nieprzydzielone — tak samo jak w przypadku niepowodzenia odzyskiwania. Aby odzyskać „utracony” wolumin, należy ponownie uruchomić zadanie. ▪ Odzyskiwanie plików lub folderów: przerwana operacja może spowodować zmiany w folderze docelowym. W zależności od czasu, jaki upłynął od momentu uruchomienia zadania, niektóre pliki mogą być odzyskane, a inne nie. Aby

Zadanie	Czynności
	odzyskać wszystkie pliki, należy ponownie uruchomić zadanie.
Edytowanie planu lub zadania	<p>Kliknij  Edytuj.</p> <p>Edycja planu tworzenia kopii zapasowych odbywa się w ten sam sposób co jego tworzenie (s. 48), z wyjątkiem następujących ograniczeń:</p> <p>Jeśli utworzone archiwum nie jest puste (czyli zawiera kopie zapasowe), podczas edycji planu tworzenia kopii zapasowych nie zawsze można używać wszystkich opcji schematów.</p> <ol style="list-style-type: none"> 1. Nie można zmienić schematu na Dziadek-ojciec-syn ani Wieża Hanoi. 2. Jeśli stosowany jest schemat Wieża Hanoi, nie jest możliwa zmiana liczby poziomów. <p>We wszystkich innych przypadkach schemat można zmienić i powinien on nadal działać tak, jakby istniejące archiwa zostały utworzone na podstawie nowego schematu. W przypadku pustych archiwów możliwe są wszystkie zmiany.</p>
Klonowanie planu tworzenia kopii zapasowych	<p>Kliknij  Klonuj.</p> <p>Klon oryginalnego planu tworzenia kopii zapasowych zostanie utworzony z domyślną nazwą „Klon <oryginalna_nazwa_planu>”. Sklonowany plan zostanie od razu wyłączony, aby nie działał równocześnie z planem oryginalnym. Ustawienia sklonowanego planu można zmienić przed jego włączeniem.</p>
Włączanie planu	<p>Kliknij  Włącz.</p> <p>Wcześniej wyłączony plan tworzenia kopii zapasowych będzie uruchamiany ponownie zgodnie z harmonogramem.</p>
Wyłączanie planu	<p>Kliknij  Wyłącz.</p> <p>Plan tworzenia kopii zapasowych nie będzie uruchamiany zgodnie z harmonogramem. Można go jednak uruchamiać ręcznie. Po ręcznym uruchomieniu plan pozostanie w dalszym ciągu wyłączony. Jeśli ponownie włączysz plan, będzie on uruchamiany jak zwykle.</p>
Eksportowanie planu	<p>Kliknij  Eksportuj.</p> <p>Określ ścieżkę i nazwę pliku wynikowego. Aby uzyskać więcej informacji, zobacz Eksportowanie oraz importowanie planów tworzenia kopii zapasowych (s. 287).</p>
Importowanie planu	<p>Kliknij  Importuj.</p> <p>Określ ścieżkę i nazwę pliku zawierającego wcześniej wyeksportowany plan. Aby uzyskać więcej informacji, zobacz Eksportowanie oraz importowanie planów tworzenia kopii zapasowych (s. 287).</p>
Usuwanie planu lub zadania	<p>Kliknij  Usuń.</p>

10.1.2 Stany i statusy planów i zadań tworzenia kopii zapasowych

Stany wykonania planu tworzenia kopii zapasowej

Stan planu tworzenia kopii zapasowych to łączny stan zadań/działań tego planu.

	Stan	Sposób ustalania	Sposób postępowania
1	Wymagające działania	Co najmniej jedno zadanie wymaga działania użytkownika. W przeciwnym razie zobacz 2.	Zidentyfikuj zadania wymagające działania (program wyświetli informacje o wymaganej czynności) -> Zatrzymaj zadania lub stwórz warunki do ich wykonywania (zmień nośnik, udostępnij dodatkowe miejsce w skarbku, zignoruj błąd odczytu, utwórz brakującą strefę Acronis Secure Zone).
2	Uruchomione	Co najmniej jedno zadanie jest uruchomione. W przeciwnym razie zobacz 3.	Nie trzeba wykonywać żadnej czynności.
3	Oczekujące	Co najmniej jedno zadanie oczekuje. W przeciwnym razie zobacz 4.	Oczekiwanie na spełnienie warunku. Ta sytuacja jest zupełnie normalna, ale zbyt długie opóźnianie tworzenia kopii zapasowej jest ryzykowne. Rozwiązaniem może być ustawienie maksymalnego opóźnienia (s. 126), po którym zadanie zostanie bezwarunkowo rozpoczęte, lub wymuszenie spełnienia warunku (poinformowanie użytkownika o konieczności wylogowania, włączenie wymaganego połączenia sieciowego). Oczekiwanie na odblokowanie niezbędnych zasobów przez inne zadanie. W odosobnionych przypadkach oczekiwanie może być konieczne, gdy z jakiegoś powodu uruchomienie zadania opóźnia się lub jego wykonywanie trwa dużo dłużej niż zwykle, co nie pozwala uruchomić innego zadania. Tego rodzaju problem znika automatycznie po zakończeniu zadania stanowiącego przeszkodę. Jeśli wykonywanie zadania trwa zbyt długo, czasem warto je zatrzymać, aby umożliwić uruchomienie następnego zadania. Trwałe nakładanie się zadań może wynikać z planu lub planów o niepoprawnym harmonogramie. W takim przypadku warto zmodyfikować plan.
4	Bezczynne	Wszystkie zadania są beczynne.	Nie trzeba wykonywać żadnej czynności.

Statusy planu tworzenia kopii zapasowych

Plan tworzenia kopii zapasowych może mieć jeden z następujących statusów: **Błąd**, **Ostrzeżenie**, **OK**.

Status planu tworzenia kopii zapasowych pochodzi z wyników ostatniego uruchomienia zadań/działań planu.

	Status	Sposób ustalania	Sposób postępowania
1	Błąd	Co najmniej jedno zadanie zakończyło się niepowodzeniem. W przeciwnym razie zobacz 2.	Zidentyfikuj zadania zakończone niepowodzeniem -> Sprawdź dziennik zadań, aby poznać przyczynę niepowodzenia, a następnie wykonaj co najmniej jedną z poniższych czynności:

			<ul style="list-style-type: none"> ■ Usuń przyczynę niepowodzenia -> [opcjonalnie] Ręcznie uruchom zadanie zakończone niepowodzeniem. ■ Jeśli niepowodzeniem zakończył się plan lokalny, zmodyfikuj go, aby zapobiec niepowodzeniu w przyszłości. ■ Jeśli niepowodzeniem zakończył się plan scentralizowany, zmodyfikuj scentralizowany plan tworzenia kopii zapasowych na serwerze zarządzania.
2	Ostrzeżenie	Co najmniej jedno zadanie zakończyło się pomyślnie z ostrzeżeniami. W przeciwnym razie zobacz 3.	Wyświetl dziennik, aby przeczytać ostrzeżenia -> [opcjonalnie] Wykonaj odpowiednie czynności, aby zapobiec ostrzeżeniom lub niepowodzeniu w przyszłości.
3	OK	Wszystkie zadania zakończyły się pomyślnie.	Nie trzeba wykonywać żadnej czynności. Należy pamiętać, że plan tworzenia kopii zapasowych może mieć status OK w przypadku, gdy nie uruchomiono jeszcze żadnych zadań.

Stany zadania

Zadanie może mieć jeden z następujących stanów wykonania: **Bezczynne**, **Oczekujące**, **Uruchomione**, **Wymagające działania**. Początkowy stan zadania to **Bezczynne**.

Po ręcznym uruchomieniu zadania lub wystąpieniu zdarzenia określonego w harmonogramie zadanie przechodzi w stan **Uruchomione** lub **Oczekujące**.

Uruchomione

Stan zadania zmienia się na **Uruchomione**, gdy wystąpi zdarzenie określone w harmonogramie, zostaną spełnione wszystkie warunki określone w planie tworzenia kopii zapasowych ORAZ nie będzie uruchomione żadne inne zadanie blokujące potrzebne zasoby. W takim przypadku nic nie stoi na przeszkodzie, aby uruchomić zadanie.

Oczekujące

Stan zadania zmienia się na **Oczekujące**, gdy zadanie ma zostać uruchomione, ale jest już wykonywane inne zadanie korzystające z tych samych zasobów. W szczególności na komputerze nie można uruchomić jednocześnie więcej niż jednego zadania tworzenia kopii zapasowej. Ponadto nie można uruchomić jednocześnie zadania tworzenia kopii zapasowej i zadania odzyskiwania, jeśli korzystają z tych samych zasobów. Gdy wykonywane zadanie odblokuje potrzebny zasób, zadanie oczekujące przejdzie w stan **Uruchomione**.

Stan zadania może także zmienić się na **Oczekujące**, gdy wystąpi zdarzenie określone w harmonogramie, ale nie zostanie spełniony warunek określony w planie tworzenia kopii zapasowych. Aby uzyskać szczegółowe informacje, zobacz Warunki uruchomienia zadania (s. 126).

Wymagające działania

Dowolne uruchomione zadanie może przejść w stan **Wymagające działania**, gdy jest konieczne działanie użytkownika, na przykład zmiana nośnika lub zignorowanie błędu odczytu. Następnym stanem może być **Bezczynne** (jeśli użytkownik wybierze zatrzymanie zadania) lub **Uruchomione** (w przypadku wybrania opcji zignorowania/ponowienia lub innej czynności — na przykład ponownego uruchomienia — która spowoduje przejście zadania w stan **Uruchomione**).

Statusy zadania

Zadanie może mieć jeden z następujących statusów: **Błąd**, **Ostrzeżenie**, **OK**.

Status zadania pochodzi z wyniku ostatniego uruchomienia zadania.

	Status	Sposób ustalania	Sposób postępowania
1	Błąd	Ostatnim wynikiem jest „Niepowodzenie”.	<p>Zidentyfikuj zadanie zakończone niepowodzeniem -> Sprawdź dziennik zadań, aby poznać przyczynę niepowodzenia, a następnie wykonaj co najmniej jedną z poniższych czynności:</p> <ul style="list-style-type: none"> ■ Usuń przyczynę niepowodzenia -> [opcjonalnie] Ręcznie uruchom zadanie zakończone niepowodzeniem. ■ Przeprowadź edycję zadania zakończonego niepowodzeniem, aby zapobiec niepowodzeniu w przyszłości.
2	Ostrzeżenie	Ostatni wynik to „Wykonane pomyślnie z ostrzeżeniami” lub wykonywanie zadania zostało zatrzymane.	Wyświetl dziennik, aby przeczytać ostrzeżenia -> [opcjonalnie] Wykonaj odpowiednie czynności, aby zapobiec ostrzeżeniom lub niepowodzeniu w przyszłości.
3	OK	Ostatni wynik to „Wykonane pomyślnie” lub „Jeszcze nie wykonane”	Stan „Jeszcze nie wykonane” oznacza, że zadanie w ogóle nie zostało uruchomione lub zostało uruchomione, ale jeszcze się nie zakończyło, więc jego wynik jest niedostępny. Czasem trzeba znaleźć przyczynę, dla której zadanie nie zostało jeszcze uruchomione.

10.1.3 Eksportowanie i importowanie planów tworzenia kopii zapasowych

Operacja eksportowania powoduje utworzenie pliku z pełną konfiguracją planu tworzenia kopii zapasowych. Plik taki można zaimportować w celu ponownego wykorzystania wyeksportowanego planu tworzenia kopii zapasowych na innym komputerze.

Scentralizowane plany tworzenia kopii zapasowych można eksportować oraz importować jedynie za pomocą serwera zarządzania.

Graficzny interfejs użytkownika programu Acronis Backup & Recovery 11 umożliwia edycję planów podczas ich importowania lub po jego zakończeniu. Plany tworzenia kopii zapasowych są eksportowane do plików .xml, które można modyfikować (s. 288) w edytorach tekstowych. Hasła w wyeksportowanych plikach są zaszyfrowane.

Przykłady użycia

- **Ponowna instalacja agenta**

Wyeksportuj plany tworzenia kopii zapasowych przed ponowną instalacją agenta, a po skończonej instalacji zaimportuj je z powrotem.

- **Wdrażanie planu tworzenia kopii zapasowych na wielu komputerach**

Dysponujesz środowiskiem, w którym nie można użyć programu Acronis Backup & Recovery 11 Management Server, na przykład z uwagi na ograniczenia zabezpieczeń. Chcesz jednak wykorzystać ten sam plan tworzenia kopii zapasowych na wielu komputerach. Wyeksportuj ten plan z jednego z komputerów i wdróż go jako plik (s. 290) na pozostałych komputerach.

Dostosowywanie poświadczeń


Plan objęty harmonogramem zawiera poświadczenia konta użytkownika, z którego są uruchamiane zadania w ramach tego planu. Plan nie zostanie uruchomiony na komputerze, na którym nie istnieje konto użytkownika o identycznych poświadczeniach. Aby uniknąć takiej sytuacji, wykonaj jedną z następujących czynności:

- Utwórz na drugim komputerze konto o identycznych poświadczeniach.
- Przed zaimportowaniem pliku eksportu przeprowadź edycję zawartych w nim poświadczeń. Aby uzyskać szczegółowe informacje, zobacz Edycja pliku eksportu (s. 288).
- Przeprowadź edycję poświadczeń po zaimportowaniu planu.


Podczas tworzenia ręcznie uruchamianego planu tworzenia kopii zapasowych nie zmieniaj ustawienia **Użyj poświadczeń bieżącego użytkownika** w sekcji **Parametry planu** > **Pokaż poświadczenia, komentarze, etykietę zadania**. Dzięki temu ustawieniu zadania w ramach planu będą zawsze wykonywane z konta użytkownika, który je uruchamia.

Kroki, które należy wykonać

Aby wyeksportować plan tworzenia kopii zapasowych

1. W widoku **Plany i zadania tworzenia kopii zapasowych** wybierz plan tworzenia kopii zapasowych.
2. Kliknij  **Eksportuj**.
3. Określ ścieżkę i nazwę pliku eksportu.
4. Potwierdź wybór.

Aby zaimportować plan tworzenia kopii zapasowych

1. W widoku **Plany i zadania tworzenia kopii zapasowych** kliknij **Importuj**. 
2. Określ ścieżkę i nazwę pliku eksportu.
3. Program Acronis Backup & Recovery 11 wyświetli stronę **Edytuj plan tworzenia kopii zapasowych**. W większości przypadków konieczna jest aktualizacja poświadczeń planu oraz poświadczeń dostępu do lokalizacji docelowej kopii zapasowej. Dokonaj wymaganych zmian i kliknij **Zapisz**. W innym razie kliknij **Anuluj**, a plan zostanie zaimportowany bez zmian.

Edycja pliku eksportu

Plik eksportu występuje w formacie .xml i można go edytować w edytorze tekstowym.

Poniżej opisano sposób wprowadzania kilku przydatnych zmian.

Jak zmodyfikować poświadczenia

Znaczniki `<login>` w pliku eksportu zawierają nazwę użytkownika, natomiast znaczniki `<password>` — jego hasło.

Aby zmodyfikować poświadczenia, zmień wartości znaczników `<login>` i `<password>` w odpowiednich sekcjach:

- poświadczenia planu — sekcja `<plan><options><common_parameters>`
- poświadczenia dostępu do danych w kopii zapasowej — sekcja `<plan><targets><inclusions>`
- poświadczenia dostępu do lokalizacji docelowej kopii zapasowej — sekcja `<plan><locations>`.

Zwróć szczególną uwagę na modyfikację znacznika `<password>`. Zawiera on zaszyfrowane hasło i ma postać `<password encrypted="true">...</password>`.

Aby zmienić zaszyfrowane hasło

1. W wierszu polecenia uruchom narzędzie `acronis_encrypt`:
`acronis_encrypt UserPassword#1`
(`UserPassword#1` to hasło, które chcesz zaszyfrować).
2. Wynikiem działania narzędzia jest ciąg, na przykład „`XXXYYZZZ888`”.
3. Skopiuj go i wklej do znacznika w następujący sposób:
`<password encrypted="true">XXXYYZZZ888</password>`

Narzędzie `acronis_encrypt` jest dostępne na każdym komputerze z zainstalowanym programem Acronis Backup & Recovery 11 Management Console. Ścieżka do narzędzia ma postać:

- `%ProgramFiles%/Common Files/Acronis/Utils` — w 32-bitowych systemach Windows
- `%ProgramFiles(x86)%/Common Files/Acronis/Utils` — w 64-bitowych systemach Windows
- `/usr/sbin` — w systemie Linux

Jak sprawić, by plan tworzenia kopii zapasowych korzystał z poświadczeń agenta

Przed rozpoczęciem importowania lub wdrażania pliku eksportu usuń wartość wymaganego znacznika `<login>`. Spowoduje to, że zaimportowany lub wdrożony plan będzie korzystał z poświadczeń usługi agenta.

Przykład

Aby sprawić, by plan tworzenia kopii zapasowych korzystał z poświadczeń agenta, znajdź znacznik `<login>` w sekcji `<plan><options><common_parameters>`. Znacznik wygląda podobnie jak ten:

```
<login>
  Administrator
</login>
<password encrypted="true">
  XXXYYZZZ888
</password>
```

Usuń wartość znacznika `<login>`, przez co znacznik przyjmie postać:

```
<login>
</login>
<password encrypted="true">
  XXXYYZZZ888
</password>
```

Jak zmienić listę elementów uwzględnianych w kopii zapasowej

Zastępowanie bezpośrednio określonego elementu innym bezpośrednio określonym elementem

W sekcji `<plan><targets><inclusions>`:

1. Usuń znacznik `<ID>`.
2. Edytuj wartość znacznika `<Path>` zawierającego informacje o danych uwzględnianych w kopii zapasowej. Na przykład, zamień „`C:`” na „`D:`”.

Zastępowanie bezpośrednio określonego elementu szablonem wyboru

W sekcji `<plan><options><specific><inclusion_rules>`:

1. Dodaj znacznik `<rules_type>` o wartości „disks” lub „files”, w zależności od typu wymaganego szablonu.
2. Dodaj znacznik `<rules>`.
3. Wewnątrz znacznika `<rules>` dodaj znacznik `<rule>` z wymaganym szablonem. Znacznik musi odpowiadać bezpośrednio określonemu elementowi. Jeśli na przykład określony element ma wartość „disks”, można użyć szablonów [SYSTEM], [BOOT] i [Fixed Volumes], ale nie można zastosować szablonu [All Files] ani [All Profiles Folder]. Aby uzyskać więcej informacji o szablonach, zobacz „Reguły wyboru woluminów” (s. 319) oraz „Reguły wyboru plików i folderów” (s. 317).
4. Aby dodać kolejny szablon, powtórz krok 3.

Przykład

Poniższy szablon ilustruje zastępowanie bezpośrednio określonego elementu szablonami wyboru.

Sekcja oryginalna:

```
<specific>
  <backup_type>
    disks
  </backup_type>
  <disk_level_options />
  <file_level_options />
  <inclusion_rules />
</specific>
```

Sekcja po zastosowaniu szablonów wyboru:

```
<specific>
  <backup_type>
    disks
  </backup_type>
  <disk_level_options />
  <file_level_options />
  <inclusion_rules>
    <rules_type>
      disks
    </rules_type>
    <rules>
      <rule>
        [BOOT]
      </rule>
      <rule>
        [SYSTEM]
      </rule>
    </rules>
  </inclusion_rules>
</specific>
```

10.1.4 Wdrażanie planów tworzenia kopii zapasowych jako plików

Przyjmijmy, że z jakiegoś powodu nie możesz uruchomić programu Acronis Backup & Recovery 11 Management Server w swoim środowisku, ale musisz zastosować jeden i ten sam plan tworzenia

kopii zapasowych w odniesieniu do wielu komputerów. Dobrym pomysłem będzie wyeksportowanie planu tworzenia kopii zapasowych z jednego komputera i wdrożenie go na wszystkich pozostałych.

Sposób działania

Na każdym komputerze z zainstalowanym agentem istnieje specjalny folder przeznaczony do przechowywania wdrożonych planów. Agent śledzi zmiany zachodzące w tym folderze. Po pojawieniu się w nim nowego pliku .xml agent zaimportuje z niego plan tworzenia kopii zapasowych. Jeśli zmienisz (lub usuniesz) plik .xml w tym specjalnym folderze, agent automatycznie zmieni (lub usunie) odpowiadający mu plan tworzenia kopii zapasowych.

Edycja pliku eksportu

Zaimportowanego w taki sposób planu tworzenia kopii zapasowych nie można edytować za pomocą graficznego interfejsu użytkownika. Możesz edytować plik eksportu (s. 288) przed wdrożeniem lub po nim za pomocą edytora tekstowego.

Jeśli wyedytujesz plik przed wdrożeniem, zmiany zostaną zastosowane na wszystkich komputerach, na których wdrożony zostanie plan. Czasem warto zmienić bezpośrednie określenie elementu do zapisania w kopii zapasowej (na przykład C: lub C:\Users) na postać szablonową (na przykład [SYSTEM] lub [All Profiles Folder]). Aby uzyskać więcej informacji o szablonach, zobacz Reguły wyboru woluminów (s. 319) oraz Reguły wyboru plików i folderów (s. 317).

Czasem warto również zmienić poświadczenia używane przez plan.

Aby wdrożyć plan tworzenia kopii zapasowych jako plik

1. Utwórz plan tworzenia kopii zapasowych na jednym z komputerów.
2. Wyeksportuj go do pliku .xml (s. 287).
3. [Opcjonalnie] Edytuj plik eksportu. Aby uzyskać więcej informacji, zobacz Edycja pliku eksportu (s. 288).
4. Wdróż ten plik .xml w specjalnym folderze.

Ścieżka do specjalnego folderu

W systemie Windows

Domyślna ścieżka do folderu specjalnego ma postać
%ALLUSERSPROFILE%\Acronis\BackupAndRecovery\import.

Jest ona przechowywana w kluczu rejestru
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\Import\folderPath.

Brak klucza oznacza, że agent nie monitoruje folderu specjalnego.

Aby zmienić ścieżkę, zmodyfikuj ten klucz. Zmiana zostanie zastosowana po ponownym uruchomieniu agenta.

W systemie Linux

Domyślna ścieżka do folderu specjalnego ma postać **/usr/lib/Acronis/BackupAndRecovery/import.**

Jest ona przechowywana w pliku **/etc/Acronis/BackupAndRecovery.config.**

Aby zmienić ścieżkę, zmień wartość **/usr/lib/Acronis/BackupAndRecovery/import** w następującym znaczniku:

```
<key name="Settings">
...
  <value name="ImportFolderPath" type="TString">
    "/usr/lib/Acronis/BackupAndRecovery/import"
  </value>
...
</key>
```

Zmiana zostanie zastosowana po ponownym uruchomieniu agenta.

Brak znacznika oznacza, że agent nie monitoruje folderu specjalnego.

10.1.5 Szczegóły planu tworzenia kopii zapasowych

W oknie **Szczegóły planu tworzenia kopii zapasowych** (wyświetlanym również w panelu **Informacje**) znajdują się wszystkie informacje dotyczące wybranego planu tworzenia kopii zapasowych.

Jeśli wykonanie planu wymaga działania użytkownika, w górnej części kart wyświetlany jest odpowiedni komunikat. Zawiera on krótki opis problemu oraz przyciski czynności umożliwiające wybór odpowiedniej czynności lub zatrzymanie planu.

Szczegóły

Karta **Plany i zadania tworzenia kopii zapasowych** zawiera następujące ogólne informacje na temat wybranego planu:

- **Nazwa** — nazwa planu tworzenia kopii zapasowych.
- **Początek** — określa, czy plan został utworzony bezpośrednio na komputerze (pochodzenie lokalne) czy wdrożony na nim za pomocą serwera zarządzania (pochodzenie centralne).
- **Stan wykonania** — stan wykonania (s. 285) planu tworzenia kopii zapasowych.
- **Status** — status (s. 285) planu tworzenia kopii zapasowych.
- **Komputer** — nazwa komputera, na którym istnieje plan tworzenia kopii zapasowych (tylko w przypadku scentralizowanych planów tworzenia kopii zapasowych).
- **Harmonogram** — określa, czy zadanie jest zaplanowane czy skonfigurowane do uruchamiania ręcznego.
- **Godzina ostatniego rozpoczęcia** — czas, który upłynął od ostatniego rozpoczęcia planu lub zadania.
- **Stan wdrażania** — stany wdrażania planów tworzenia kopii zapasowych (tylko w przypadku scentralizowanych planów tworzenia kopii zapasowych).
- **Godzina ostatniego zakończenia** — czas, który upłynął od ostatniego zakończenia planu lub zadania.
- **Ostatni wynik** — wynik ostatniego uruchomienia planu lub zadania.
- **Typ** — typ planu lub zadania tworzenia kopii zapasowych.
- **Właściciel** — nazwa użytkownika, który utworzył lub jako ostatni zmodyfikował plan.
- **Godzina następnego rozpoczęcia** — godzina następnego uruchomienia planu lub zadania.
- **Komentarze** — opis planu (jeśli podano).

Zadań

Karta **Zadania** zawiera listę wszystkich zadań wybranego planu tworzenia kopii zapasowych. Aby wyświetlić szczegółowe informacje na temat wybranego zadania, kliknij **Szczegóły**.

Postęp

Na karcie **Postęp** znajduje się lista wszystkich aktualnie uruchomionych lub oczekujących na uruchomienie czynności związanych z wybranym planem tworzenia kopii zapasowych.

Historia

Karta **Historia** umożliwia śledzenie historii wszystkich zakończonych czynności w ramach planu tworzenia kopii zapasowych.

Elementy uwzględniane w kopii zapasowej

Karta **Źródło** zawiera następujące informacje na temat danych wybranych do utworzenia kopii zapasowej:

- **Typ źródła** — typ danych wybranych do utworzenia kopii zapasowej.
- **Elementy uwzględniane w kopii zapasowej** — elementy wybrane do utworzenia kopii zapasowej i ich rozmiar.

Miejsce docelowe kopii zapasowej

Karta **Miejsce docelowe** zawiera następujące informacje:

- **Nazwa** — nazwa archiwum.
- **Lokalizacja** — nazwa skarbca lub ścieżka do folderu, w którym jest przechowywane archiwum.
- **Komentarze dotyczące archiwum** — komentarze na temat archiwum (jeśli podano).
- **2. lokalizacja, 3. lokalizacja, 4. lokalizacja, 5. lokalizacja** — nazwy lokalizacji, do których skopiowano lub przeniesiono archiwum (jeśli określono w planie tworzenia kopii zapasowych).

Ustawienia

Karta **Ustawienia** zawiera następujące informacje:

- **Schemat tworzenia kopii zapasowych** — wybrany schemat tworzenia kopii zapasowych i wszystkie jego ustawienia z harmonogramami.
- **Sprawdzanie poprawności** (jeśli określono) — zdarzenia, przed którymi lub po których wykonywane jest sprawdzanie poprawności, a także harmonogram tej operacji. Jeśli parametr sprawdzania poprawności nie został ustawiony, będzie wyświetlana wartość **Nigdy**.
- **Opcje tworzenia kopii zapasowej** — opcje tworzenia kopii zapasowych zmienione w porównaniu z wartościami domyślnymi.

10.1.6 Szczegóły zadania/działania

Na kilku kartach w oknie **Szczegóły zadania/działania** (wyświetlanym również w panelu **Informacje**) znajdują się wszystkie informacje o wybranym zadaniu lub działaniu.

Gdy zadanie lub działanie wymaga działania użytkownika, nad kartami pojawi się komunikat wraz z przyciskami czynności. Komunikat zawiera krótki opis problemu. Przyciski umożliwiają ponowne uruchomienie lub zatrzymanie zadania bądź działania.

10.2 Dziennik

Dziennik zawiera historię operacji wykonywanych na komputerze przez program Acronis Backup & Recovery 11.

Aby wyświetlić zwykłą listę wpisów dziennika, wybierz **Zdarzenia** z listy rozwijanej **Wyświetlaj**. Aby wyświetlić wpisy dziennika pogrupowane według działań, wybierz **Działania**. Szczegółowe informacje na temat wybranego wpisu dziennika lub działania są wyświetlane w panelu **Informacje** w dolnej części widoku **Dziennik**.



Aby wyświetlić żądane działania i wpisy dziennika w tabeli, skorzystaj z filtrów. Możesz również ukrywać niepotrzebne kolumny i wyświetlać kolumny ukryte. Aby uzyskać szczegółowe informacje, zobacz „Sortowanie, filtrowanie i konfigurowanie elementów tabeli” (s. 26).




Wybierz żądane działanie lub wpis, aby wykonać związaną z nim czynność. Aby uzyskać szczegółowe informacje, zobacz „Czynności dotyczące wpisów dziennika” (s. 294) oraz „Szczegóły wpisu dziennika” (s. 295).

10.2.1 Czynności dotyczące wpisów dziennika

Wszystkie operacje opisane poniżej wykonuje się przez kliknięcie odpowiednich elementów na **pasku narzędzi** dziennika. Operacje te można również wykonać za pomocą menu kontekstowego (klikając prawym przyciskiem myszy wpis dziennika lub działanie)

Poniżej przedstawiono wytyczne dotyczące wykonywania czynności związanych z wpisami dziennika.

Zadanie	Czynności
Wybieranie pojedynczego działania	Z listy rozwijanej Wyświetlaj wybierz Działania i kliknij działanie. Panel Informacje będzie zawierał wpisy dziennika dotyczące wybranego działania.
Wybieranie pojedynczego wpisu dziennika	Kliknij wpis.
Wybieranie wielu wpisów dziennika	<ul style="list-style-type: none"> ▪ <i>Niesąsiadujące</i>: przytrzymaj klawisz CTRL i pojedynczo klikaj żądane wpisy dziennika. ▪ <i>Sąsiadujące</i>: wybierz jeden wpis dziennika, a następnie przytrzymaj klawisz SHIFT i kliknij inny wpis dziennika. Wszystkie wpisy dziennika między pierwszym a ostatnim również zostaną wybrane.
Wyświetlanie szczegółów wpisu dziennika	<ol style="list-style-type: none"> 1. Wybierz wpis dziennika. 2. Wykonaj jedną z następujących czynności: <ul style="list-style-type: none"> ▪ Kliknij dwukrotnie zaznaczenie. ▪ Kliknij  Szczegóły. <p>Zostaną wyświetlone szczegóły wpisu dziennika. Aby poznać szczegółowe informacje dotyczące działań związanych z wpisami dziennika, zobacz Szczegóły wpisu dziennika (s. 353).</p>
Zapisywanie wybranych wpisów dziennika w pliku	<ol style="list-style-type: none"> 1. Wyświetl Działania i wybierz działania lub wyświetl Zdarzenia i wybierz wpisy dziennika. 2. Kliknij  Zapisz zaznaczone w pliku. 3. W otwartym oknie określ ścieżkę i nazwę pliku. <p>W określonym pliku zostaną zapisane wszystkie wpisy dziennika dotyczące wybranych działań lub wybrane wpisy dziennika.</p>

Zapisywanie wszystkich wpisów dziennika w pliku	<ol style="list-style-type: none"> 1. Upewnij się, że nie są ustawione żadne filtry. 2. Kliknij  Zapisz wszystko w pliku. 3. W otwartym oknie określ ścieżkę i nazwę pliku. W określonym pliku zostaną zapisane wszystkie wpisy dziennika.
Zapisywanie wszystkich odfiltrowanych wpisów dziennika w pliku	<ol style="list-style-type: none"> 1. Ustaw filtry tak, aby uzyskać listę wpisów dziennika spełniających kryteria filtrowania. 2. Kliknij  Zapisz wszystko w pliku. 3. W otwartym oknie określ ścieżkę i nazwę pliku. <p>W określonym pliku zostaną zapisane wszystkie wpisy dziennika z listy.</p>
Usuwanie wszystkich wpisów dziennika	<p>Kliknij  Wyczyść dziennik.</p> <p>Wszystkie wpisy dziennika zostaną usunięte z dziennika i zostanie utworzony nowy wpis dziennika. Będzie on zawierał informację o tym, kto i kiedy usunął wpisy dziennika.</p>

10.2.2 Szczegóły wpisu dziennika

W tym miejscu wyświetlane są szczegółowe informacje dotyczące wybranego wpisu dziennika. Informacje te można skopiować do schowka.

Aby wyświetlić szczegółowe informacje na temat następnego lub poprzedniego wpisu dziennika, kliknij odpowiednio przycisk strzałki w dół lub w górę.

Aby skopiować szczegóły, kliknij przycisk **Kopiuj do schowka**.

Pola danych wpisu dziennika

Wpis dziennika zawiera następujące pola danych:

- **Typ** — typ zdarzenia (Błąd, Ostrzeżenie, Informacja).
- **Data i godzina** — data i godzina wystąpienia zdarzenia.
- **Plan tworzenia kopii zapasowych** — plan tworzenia kopii zapasowych, z którym związane jest zdarzenie (jeśli dotyczy).
- **Zadanie** — zadanie, z którym związane jest zdarzenie (jeśli dotyczy).
- **Kod** — wartość pusta lub kod błędu programu, jeśli typem zdarzenia jest błąd. Kod błędu to liczba całkowita, która może posłużyć działowi pomocy technicznej firmy Acronis do rozwiązania problemu.
- **Moduł** — wartość pusta lub numer modułu programu, w którym wystąpił błąd. Jest to liczba całkowita, która może posłużyć działowi pomocy technicznej firmy Acronis do rozwiązania problemu.
- **Właściciel** — nazwa użytkownika będącego właścicielem (s. 32) planu tworzenia kopii zapasowych.
- **Komunikat** — tekstowy opis zdarzenia.

Sposób wyświetlania daty i godziny zależy od ustawień lokalnych.

10.3 Alerty

Alert to komunikat ostrzegawczy informujący o rzeczywistych lub potencjalnych problemach. Widok **Alerty** pozwala na błyskawiczną identyfikację i rozwiązywanie problemów, umożliwiając monitorowanie bieżących alertów i podgląd ich historii.

Alerty aktywne i nieaktywne

Alert może znajdować się w stanie aktywnym lub nieaktywnym. Stan aktywny oznacza, że problem, który go wywołał, w dalszym ciągu istnieje. Alert staje się nieaktywny, gdy problem, który go wywołał, został ręcznie lub samoistnie rozwiązany.

Uwaga: *Jeden rodzaj alertu pozostaje zawsze aktywny: „Nie utworzono kopii zapasowej”. Wiąże się to z faktem, iż nawet po rozwiązaniu przyczyny alertu i pomyślnym utworzeniu kolejnych kopii zapasowych problem dotyczący nieutworzenia kopii zapasowej w dalszym ciągu istnieje.*

Naprawianie błędów, które wywołały alerty

Aby znaleźć i naprawić problem, który wywołał alert, kliknij **Napraw problem**. Nastąpi przeniesienie do odpowiedniego widoku, gdzie można przeanalizować problem i podjąć niezbędne kroki naprawcze.

Opcjonalnie można kliknąć **Wyświetl szczegóły** i uzyskać pełniejsze informacje na temat zaznaczonego alertu.

Akceptowanie alertów

Domyślnie w tabeli **Bieżące alerty** znajdują się zarówno aktywne, jak i nieaktywne alerty do czasu ich zaakceptowania. Aby zaakceptować alert, zaznacz go i kliknij **Zaakceptuj**. Przez zaakceptowanie alertu przyjmujesz do wiadomości fakt jego wystąpienia i zgadzasz się na przyjęcie za niego odpowiedzialności. Zaakceptowane alerty są przenoszone do tabeli **Zaakceptowane alerty** z niezmienioną informacją o ich stanie.

W tabeli **Zaakceptowane alerty** jest przechowywana historia zaakceptowanych alertów. Umożliwia ona ustalenie osoby, która zaakceptowała dany alert, oraz daty i godziny tego zdarzenia. Zaakceptowane alerty w obu stanach można usuwać z tabeli ręcznie — za pomocą przycisków **Usuń** oraz **Usuń wszystkie**, lub automatycznie (zobacz „Konfigurowanie alertów” w dalszej części tej sekcji).

Aby wyeksportować pełną zawartość tabeli do pliku *.txt lub *.csv, kliknij **Zapisz wszystko w pliku**.

Konfigurowanie alertów

Do konfigurowania alertów służą następujące opcje dostępne w górnej części widoku **Alerty**:

- **Pokaż/ukryj alerty** (s. 29) — określenie typów alertów wyświetlanych w widoku **Alerty**.
- **Powiadomienia** (s. 299) — konfiguracja powiadomień e-mail o zgłaszanych alertach.
- **Ustawienia** (s. 297) — możliwość określenia, czy nieaktywne alerty mają być automatycznie przenoszone do tabeli **Zaakceptowane alerty**, oraz wskazania okresu przechowywania zaakceptowanych alertów w tabeli **Zaakceptowane alerty**.

10.4 Zbieranie informacji o systemie

Narzędzie do zbierania informacji o systemie pozwala zebrać informacje o komputerze, do którego podłączona jest konsola zarządzania, a następnie zapisać je do pliku. Plikiem tym warto dysponować podczas kontaktu z działem pomocy technicznej firmy Acronis.

Ta opcja jest dostępna na nośniku startowym oraz na komputerach, na których zainstalowano agenta dla systemu Windows lub Linux albo serwer Acronis Backup & Recovery 11 Management Server.

Aby zebrać informacje o systemie

1. W konsoli zarządzania wybierz w górnym menu kolejno **Pomoc > Zbierz informacje o systemie** z „nazwa komputera”.
2. Określ plik, do którego chcesz zapisać informacje o systemie.

10.5 Dostosowywanie opcji komputera

Opcje komputera określają ogólne zachowanie wszystkich agentów Acronis Backup & Recovery 11 działających na zarządzanym komputerze, w związku z czym są one odrębne dla każdego komputera.

Aby uzyskać dostęp do opcji komputera, należy podłączyć konsolę do komputera zarządzanego, a następnie z górnego menu wybrać **Opcje > Opcje komputera**.

10.5.1 Program jakości obsługi klienta

Ta opcja określa, czy komputer zostanie objęty Programem jakości obsługi klienta firmy Acronis (ACEP).

Jeśli wybierzesz opcję **Tak, chcę wziąć udział w programie ACEP**, informacje o konfiguracji sprzętowej, najczęściej i najrzadziej używanych funkcjach oraz wszelkich problemach będą automatycznie zbierane z komputera i regularnie wysyłane do firmy Acronis. Wyniki końcowe posłużą do udoskonalenia i zwiększenia funkcjonalności oprogramowania w celu lepszego dostosowania go do potrzeb klientów firmy Acronis.

Firma Acronis nie zbiera żadnych danych osobowych. Aby dowiedzieć się więcej na temat programu ACEP, przeczytaj warunki udziału w witrynie internetowej firmy Acronis lub w graficznym interfejsie użytkownika zainstalowanego programu.

Na początku opcja jest konfigurowana podczas instalacji agenta Acronis Backup & Recovery 11. Ustawienie to można zmienić w dowolnym momencie, korzystając z graficznego interfejsu użytkownika (**Opcje > Opcje komputera > Program jakości obsługi klienta**). Opcję można również skonfigurować przy użyciu przystawki Zasady grupy (s. 371). Ustawienia określonego za pomocą zasad grupy nie można zmienić w graficznym interfejsie użytkownika programu, chyba że na komputerze zostaną wyłączone zasady grupy.

10.5.2 Alerty

Zarządzanie alertami

Usuwanie z kategorii „Zaakceptowane alerty” elementy starsze niż

Ta opcja pozwala określić, czy zaakceptowane alerty mają być usuwane z tabeli **Zaakceptowane alerty**.

Ustawienie wstępne: **Wyłączone**.

Włączenie opcji umożliwia określenie okresu przechowywania zaakceptowanych alertów. Zaakceptowane alerty starsze niż wskazany okres będą automatycznie usuwane z tabeli.

Automatycznie przenoś nieaktywne alerty do kategorii „Zaakceptowane alerty”

Opcja ta pozwala określić, czy wszystkie alerty, które stają się nieaktywne, mają być automatycznie akceptowane i przenoszone do tabeli **Zaakceptowane alerty**.

Ustawienie wstępne: **Wyłączone**.

Włączenie opcji umożliwia określenie typów alertów, do których ma ona mieć zastosowanie.

Alerty związane z czasem

Ostatnia kopia zapasowa

Ta opcja jest dostępna, gdy konsola jest podłączona do komputera zarządzanego (s. 380) lub serwera zarządzania (s. 384).

Określa ona, czy ma być wyświetlany alert w przypadku, gdy na danym komputerze od pewnego czasu nie została utworzona kopia zapasowa. Można określić czas krytyczny z punktu widzenia firmy.

Ustawienie wstępne: alert w przypadku, gdy ostatnia kopia zapasowa na komputerze została pomyślnie utworzona ponad **5 dni** temu.

Alert jest wyświetlany w widoku **Alerty** w panelu **Nawigacja**. Gdy konsola jest podłączona do serwera zarządzania, to ustawienie określa również schemat kolorów dla wartości odpowiadających poszczególnym komputerom w kolumnie **Ostatnia kopia zapasowa**.

Ostatnie połączenie

Ta opcja jest dostępna, gdy konsola jest podłączona do serwera zarządzania lub do zarejestrowanego komputera (s. 380).

Określa ona, czy ma być wyświetlany alert w przypadku, gdy przez pewien czas nie zostanie nawiązane połączenie między zarejestrowanym komputerem a serwerem zarządzania, co oznacza, że komputer może nie być centralnie zarządzany (na przykład w przypadku błędu połączenia sieciowego z tym komputerem). Można skonfigurować czas uważany za krytyczny.

Ustawienie wstępne: alert w przypadku, gdy ostatnie połączenie komputera z serwerem zarządzania nastąpiło ponad **5 dni** temu.

Alert jest wyświetlany w widoku **Alerty** w panelu **Nawigacja**. Gdy konsola jest podłączona do serwera zarządzania, to ustawienie określa również schemat kolorów dla wartości odpowiadających poszczególnym komputerom w kolumnie **Ostatnie połączenie**.

10.5.3 Powiadomienia pocztą e-mail

Ta opcja umożliwia konfigurowanie powiadomień e-mail.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować powiadamianie pocztą e-mail

1. W polu **Serwer SMTP** wprowadź nazwę serwera SMTP.
2. W polu **Port** ustaw port serwera SMTP. Domyślnie jest to port 25.

3. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika.
4. W polu **Hasło** wprowadź hasło.
5. Kliknij **Dodatkowe parametry poczty e-mail**, aby skonfigurować przedstawione poniżej parametry poczty e-mail, a następnie kliknij **OK**:
 - **Od** — wpisz adres e-mail użytkownika, od którego zostanie wysłana wiadomość. Jeśli pozostawisz to pole puste, wiadomości będą tworzone w taki sposób, jakby pochodziły z adresu docelowego.
 - **Użyj szyfrowania** — umożliwia włączenie szyfrowanego połączenia z serwerem poczty. Można wybrać szyfrowanie SSL lub TLS.
 - Niektórzy dostawcy usług internetowych umożliwiają wysłanie poczty dopiero po uwierzytelnieniu na serwerze poczty przychodzącej. Jeśli tak jest, zaznacz pole wyboru **Zaloguj się na serwerze poczty przychodzącej**, aby umożliwić korzystanie z serwera POP i skonfigurować jego ustawienia:
 - **Serwer poczty przychodzącej (POP)** — wprowadź nazwę serwera POP.
 - **Port** — ustaw port serwera POP. Domyślnie jest to port **110**.
 - **Nazwa użytkownika** — wprowadź nazwę użytkownika.
 - **Hasło** — wprowadź hasło.
6. Kliknij **OK**.

Powiadomienia o alertach

Program Acronis Backup & Recovery 11 umożliwia powiadamianie użytkowników o alertach w formie wiadomości e-mail.

Opcja ta umożliwia określenie godziny i częstotliwości otrzymywania powiadomień o określonych typach alertów.

Ustawienie wstępne: **Wyłączone**.

Uwaga: Przed rozpoczęciem konfigurowania powiadomień o alertach należy określić ustawienia serwera SMTP w sekcji *Powiadomienia pocztą e-mail* (s. 298).

Aby skonfigurować powiadomienia o alertach

1. Zaznacz pole wyboru **Wysyłaj powiadomienia pocztą e-mail**.
2. W polu **Adresy e-mail** wpisz adres e-mail, na który będą wysyłane powiadomienia. Można wprowadzić kilka adresów oddzielonych średnikami.
3. W polu **Temat** wpisz temat wiadomości z powiadomieniem lub pozostaw wartość domyślną.
4. Wybierz wymaganą metodę wysyłania powiadomień:
 - Każdy alert — powiadomienia będą wysyłane natychmiast po odebraniu nowego alertu:
 - Zaznacz pole wyboru **Natychmiast po wystąpieniu alertu**.
 - Kliknij **Wybierz typy alertów...**, aby określić typy alertów, o których chcesz otrzymywać powiadomienia.
 - Według harmonogramu — powiadomienie obejmujące wszystkie alerty, jakie wystąpiły w danym okresie. Aby otrzymywać powiadomienia według harmonogramu:
 - Zaznacz pole wyboru **Według harmonogramu**.
 - Kliknij **Wybierz typy alertów...**, aby określić typy alertów, o których chcesz otrzymywać powiadomienia.
 - Kliknij **Harmonogram powiadomień**, aby skonfigurować częstotliwość i godzinę wysyłania powiadomień.

5. Kliknij **OK**.
6. Kliknij **Wyślij próbną wiadomość e-mail**, aby sprawdzić, czy ustawienia są poprawne.

10.5.4 Śledzenie zdarzeń

Zdarzenia z dziennika generowane przez agenty działające na komputerze zarządzanym można duplikować w dzienniku zdarzeń aplikacji systemu Windows lub wysyłać do określonych menedżerów SNMP. Jeśli opcje śledzenia zdarzeń nie zostaną zmodyfikowane w żadnym innym miejscu, ustawienia określone tutaj będą stosowane do każdego lokalnego planu utworzenia kopii zapasowych i każdego zadania utworzonego na komputerze.

Określone tutaj ustawienia można zastąpić — wyłącznie dla zdarzeń występujących podczas tworzenia kopii zapasowych lub odzyskiwania — w sekcji Domyślne opcje tworzenia kopii zapasowej i odzyskiwania. W takim przypadku ustawienia określone tutaj będą stosowane do operacji innych niż tworzenie kopii zapasowych i odzyskiwanie, takich jak sprawdzanie poprawności lub czyszczenie archiwum.

Ponadto podczas definiowania planu tworzenia kopii zapasowych lub zadania odzyskiwania można zastąpić ustawienia określone w domyślnych opcjach tworzenia kopii zapasowych i odzyskiwania. Uzyskane w ten sposób ustawienia będą dotyczyły konkretnego planu lub zadania.

Powiadomienia SNMP

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa, czy agenty działające na komputerze zarządzanym muszą wysyłać zdarzenia z dziennika do określonych menedżerów Simple Network Management Protocol (SNMP). Można wybrać typy wysyłanych zdarzeń.

Określone tutaj ustawienia można zastąpić w przypadku zdarzeń występujących podczas tworzenia kopii zapasowych lub odzyskiwania, w sekcji Domyślne opcje tworzenia kopii zapasowej i odzyskiwania. W takim przypadku określone tutaj ustawienia będą uwzględniane w przypadku operacji innych niż tworzenie kopii zapasowych i odzyskiwanie, na przykład podczas sprawdzania poprawności archiwum lub czyszczenia.

Podczas tworzenia planu tworzenia kopii zapasowych lub zadania odzyskiwania można również zastąpić ustawienia określone w domyślnych opcjach tworzenia kopii zapasowej i odzyskiwania. Uzyskane w ten sposób ustawienia będą dotyczyły konkretnego planu lub zadania.

Aby uzyskać szczegółowe informacje na temat programu Acronis Backup & Recovery 11, zobacz „Obsługa SNMP (s. 46)”.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować wysyłanie komunikatów SNMP

1. Zaznacz pole wyboru **Wysyłaj wiadomości do serwera SNMP**.
2. Określ odpowiednie opcje:
 - **Typy wysyłanych zdarzeń** — wybierz typy zdarzeń: **Wszystkie zdarzenia, Błędy i ostrzeżenia** lub **Tylko błędy**.
 - **Nazwa/adres IP serwera** — wpisz nazwę lub adres IP hosta, na którym uruchomiona jest aplikacja zarządzająca SNMP, do której chcesz wysyłać komunikaty.

- **Spółeczność** — wpisz nazwę społeczności SNMP, do której należy host z aplikacją zarządzającą SNMP oraz komputer wysyłający. Typowe ustawienie to „public” („publiczna”).

Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy ustawienia są poprawne.

Aby wyłączyć wysyłanie komunikatów SNMP, wyczyść pole wyboru **Wysyłaj wiadomości do serwera SNMP**.

Komunikaty są wysyłane przy użyciu protokołu UDP.

Następna sekcja zawiera dodatkowe informacje na temat Konfigurowanie usług SNMP na komputerze odbierającym (s. 301).

Konfigurowanie usług SNMP na komputerze odbierającym

Windows

Aby zainstalować usługę SNMP na komputerze z systemem Windows:

1. **Start > Panel sterowania > Dodaj lub usuń programy > Dodaj/Usuń składniki systemu Windows.**
2. Wybierz **Narzędzia zarządzania i monitorowania**.
3. Kliknij **Szczegóły**.
4. Zaznacz pole wyboru **Protokół Simple Network Management Protocol**.
5. Kliknij **OK**.

Może zostać wyświetlony monit o plik Immib2.dll, który znajduje się na płycie instalacyjnej systemu operacyjnego.

Linux

W celu odbierania komunikatów SNMP na komputerze z systemem Linux należy zainstalować pakiet net-snmp (w przypadku dystrybucji RHEL i SUSE) lub snmpd (w przypadku dystrybucji Debian).

Protokół SNMP można skonfigurować przy użyciu polecenia **snmpconf**. Domyślne pliki konfiguracyjne znajdują się w katalogu `/etc/snmp`:

- `/etc/snmp/snmpd.conf` — plik konfiguracyjny agenta SNMP Net-SNMP,
- `/etc/snmp/snmptrapd.conf` — plik konfiguracyjny demona pułapki Net-SNMP.

Dziennik zdarzeń systemu Windows

Ta opcja jest uwzględniana tylko w systemach operacyjnych Windows.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa, czy agenty działające na komputerze zarządzanym muszą rejestrować zdarzenia w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, uruchom program **eventvwr.exe** lub wybierz kolejno: **Panel sterowania > Narzędzia administracyjne > Podgląd zdarzeń**). Zarejestrowane zdarzenia można filtrować.

Określone tutaj ustawienia można zastąpić w przypadku zdarzeń występujących podczas tworzenia kopii zapasowych lub odzyskiwania, w sekcji Domyślne opcje tworzenia kopii zapasowej i odzyskiwania. W takim przypadku określone tutaj ustawienia będą uwzględniane w przypadku operacji innych niż tworzenie kopii zapasowych i odzyskiwanie, na przykład podczas sprawdzania poprawności archiwum lub czyszczenia.

Podczas tworzenia planu tworzenia kopii zapasowych lub zadania odzyskiwania można również zastąpić ustawienia określone w domyślnych opcjach tworzenia kopii zapasowej i odzyskiwania. Uzyskane w ten sposób ustawienia będą dotyczyły konkretnego planu lub zadania.

Wstępnie ustawiona wartość: **Wyłączone**.

Aby wyłączyć tę opcję, zaznacz pole wyboru **Rejestruj zdarzenia**.

Pole wyboru **Typy rejestrowanych zdarzeń** umożliwia filtrowanie zdarzeń rejestrowanych w dzienniku zdarzeń aplikacji systemu Windows:

- **Wszystkie zdarzenia** — wszystkie zdarzenia (informacje, ostrzeżenia i błędy);
- **Błędy i ostrzeżenia;**
- **Tylko błędy.**

Aby wyłączyć tę opcję, anuluj zaznaczenie pola wyboru **Rejestruj zdarzenia**.

10.5.5 Reguły czyszczenia dziennika

Ta opcja określa sposób czyszczenia dziennika agenta Acronis Backup & Recovery 11.

Ta opcja definiuje maksymalny rozmiar folderu z dziennikiem agenta (który w przypadku systemów Windows XP/2003 znajduje się w katalogu %ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\LogEvents).

Ustawienie wstępne: **Maksymalny rozmiar dziennika: 50 MB. Podczas czyszczenia zachowaj 95% maksymalnego rozmiaru dziennika.**

Po włączeniu tej opcji program będzie co 100 pozycji dziennika porównywał jego bieżący rozmiar z rozmiarem maksymalnym. Gdy maksymalny rozmiar dziennika zostanie przekroczony, program usunie najstarsze pozycje. Istnieje możliwość ustawienia liczby pozycji, które mają być zachowane. Ustawienie domyślne (95%) oznacza zachowanie większości dziennika. Ustawienie minimalne (1%) oznacza praktycznie wyczyszczenie dziennika.

Parametr ten można także ustawić za pomocą szablonu Acronis Administrative Template (s. 361).

10.5.6 Zarządzanie komputerem

Ta opcja określa, czy komputer ma być zarządzany centralnie przez serwer zarządzania Acronis Backup & Recovery 11 Management Server.

Aby móc używać tej opcji, należy zalogować się jako członek grupy **Administratorzy** na komputerze.

Komputer można zarejestrować na serwerze zarządzania podczas instalowania agenta programu Acronis Backup & Recovery 11. Jeśli komputer nie jest zarejestrowany, wybranie opcji **Zarządzanie scentralizowane** spowoduje zainicjowanie rejestracji (s. 383). Komputer można również dodać do serwera zarządzania po stronie samego serwera. Każda z tych trzech metod rejestracji wymaga uprawnień administratora serwera.

Wybranie na zarejestrowanym komputerze opcji **Zarządzanie autonomiczne** spowoduje wstrzymanie jego komunikacji z serwerem. Na serwerze zarządzania komputer jest wyświetlany jako **Wycofany**. Administrator serwera zarządzania może usunąć komputer z serwera lub zarejestrować go ponownie.

Ustawienie wstępne: **Zarządzanie autonomiczne.**

Aby na komputerze skonfigurować zarządzanie scentralizowane:

1. Wybierz **Zarządzanie scentralizowane**.
2. Określ dane w obszarze **Serwer zarządzania (IP/nazwa)**.
3. Po wyświetleniu monitu określ nazwę użytkownika i hasło administratora serwera zarządzania.
4. W polu **Adres rejestracji komputera** wybierz sposób rejestracji serwera zarządzania: wg jego nazwy (sposób zalecany) lub jego adresu IP.
5. Kliknij **OK**. Komputer zostanie zarejestrowany na serwerze zarządzania.

Aby wyłączyć zarządzanie scentralizowane, należy wybrać **Zarządzanie autonomiczne**.

10.5.7 Serwer proxy kopii zapasowej online

Ta opcja jest dostępna tylko w przypadku tworzenia kopii zapasowej oraz odzyskiwania jej z magazynu Acronis Online Backup Storage za pośrednictwem Internetu.

Ta opcja określa, czy agent Acronis ma łączyć się z Internetem za pośrednictwem serwera proxy.

Uwaga: Funkcja Acronis Backup & Recovery Online obsługuje wyłącznie serwery proxy HTTP i HTTPS.

Aby skonfigurować ustawienia serwera proxy

1. Zaznacz pole wyboru **Użyj serwera proxy**.
2. W polu **Adres** określ nazwę sieciową lub adres IP serwera proxy — na przykład: **proxy.example.com** lub **192.168.0.1**
3. W polu **Port** określ numer portu serwera proxy — na przykład: **80**
4. Jeśli serwer proxy wymaga uwierzytelniania, określ poświadczenia w polach **Nazwa użytkownika** i **Hasło**.
5. Aby sprawdzić poprawność ustawień serwera proxy, kliknij **Sprawdź połączenie**.

Jeżeli nie znasz ustawień serwera proxy, skontaktuj się z administratorem sieci lub usługodawcą internetowym w celu uzyskania pomocy.

Możesz także posłużyć się ustawieniami z konfiguracji przeglądarki internetowej. Oto informacje ułatwiające odnalezienie ich w trzech popularnych przeglądarkach.

- **Microsoft Internet Explorer.** W menu **Narzędzia** kliknij **Opcje internetowe**. Na karcie **Połączenia** kliknij **Ustawienia sieci LAN**.
- **Mozilla Firefox.** W menu **Narzędzia** kliknij **Opcje**, a następnie kliknij **Zaawansowane**. Na karcie **Sieć** w obszarze **Połączenie** kliknij **Ustawienia**.
- **Google Chrome.** W oknie **Opcje** kliknij **Dla zaawansowanych**. W obszarze **Sieć** kliknij **Zmień ustawienia proxy**.

11 Zarządzanie scentralizowane

W tej sekcji opisano operacje, które można wykonać centralnie przy użyciu składników do zarządzania scentralizowanego. Zawartość niniejszej sekcji dotyczy wyłącznie zaawansowanych wersji programu Acronis Backup & Recovery 11.

11.1 Opis zarządzania scentralizowanego

Ta sekcja zawiera omówienie scentralizowanej ochrony danych przy użyciu programu Acronis Backup & Recovery 11. Przed lekturą tej sekcji należy zapoznać się z metodami ochrony danych na jednym komputerze.

11.1.1 Podstawowe pojęcia

Tworzenie scentralizowanych planów tworzenia kopii zapasowych i śledzenie ich wykonywania

Aby chronić dane na jednym komputerze, należy zainstalować na nim agenta (s. 376) lub kilka agentów do różnych typów danych, które wymagają ochrony. Do komputera można podłączyć konsolę i skonfigurować plan tworzenia kopii zapasowych (s. 382) lub kilka takich planów.

Co jednak zrobić w przypadku konieczności zarządzania setkami komputerów? Zdefiniowanie planu tworzenia kopii zapasowych na każdym komputerze wymaga czasu, nawet jeśli plany są podobne — na przykład przewidują tworzenie kopii zapasowej dysku systemowego i dokumentów użytkowników. Czasochłonne jest również śledzenie wykonywania planów na poszczególnych komputerach.

Aby uzyskać możliwość rozprzestrzeniania operacji zarządzania na wiele komputerów, należy zainstalować serwer Acronis Backup & Recovery 11 Management Server (s. 384) i zarejestrować (s. 383) na nim komputery. Następnie można utworzyć grupy komputerów, aby umożliwić jednoczesne zarządzanie wieloma komputerami. Wszystkie komputery lub ich wybrany zbiór można chronić, konfigurując scentralizowany plan tworzenia kopii zapasowych (s. 315).

Po skonfigurowaniu na serwerze zarządzania scentralizowanego planu tworzenia kopii zapasowych serwer wdraża go na wszystkich komputerach objętych planem. Agenty na komputerach rozpoczną wykonywanie planu. Status planu można monitorować na jednym ekranie, przechodząc w razie potrzeby do poszczególnych komputerów lub działań, aby sprawdzić ich status i wpisy dziennika. Serwer zarządzania umożliwia także monitorowanie lokalnie inicjowanych działań agenta i zarządzanie nimi.

Ponieważ konsolę podłącza się do serwera zarządzania, a nie do poszczególnych komputerów, a wszystkie operacje wykonuje się za pośrednictwem centralnej jednostki zarządzania, ten sposób zarządzania określa się jako zarządzanie scentralizowane (s. 389).

Zarządzanie scentralizowane (s. 389) nie wyklucza bezpośredniego zarządzania każdym komputerem. Konsolę można podłączać do poszczególnych komputerów w celu wykonania dowolnych operacji zarządzania bezpośredniego. Jednak zarządzanie scentralizowanymi planami tworzenia kopii zapasowych jest możliwe tylko z poziomu serwera zarządzania, ponieważ dobrze przemyślane funkcje planu działają automatycznie i rzadko wymagają interwencji człowieka.

Korzystając z serwera zarządzania, można utworzyć jeden lub więcej scentralizowanych magazynów archiwów (skarbców centralnych (s. 385)), które będą współużytkowane przez zarejestrowane

komputery. Skarbiec centralny może być używany przez dowolny plan tworzenia kopii zapasowych, centralny lub utworzony na zarejestrowanych komputerach przy użyciu funkcji zarządzania bezpośredniego.

Organizowanie zarządzanego archiwum pamięci masowej

Jaka powinna być pojemność skarbca centralnego? Czy przesyłanie do skarbca dużych kopii zapasowych nie spowoduje przeciążenia sieci? Czy kopia zapasowa serwera produkcyjnego tworzona w trybie online wpływa na jego wydajność? Aby scentralizowane tworzenie kopii zapasowych nie spowalniało procesów biznesowych w firmie, a także aby zminimalizować ilość zasobów wymaganych do ochrony danych, należy zainstalować węzeł magazynowania Acronis Backup & Recovery 11 Storage Node (s. 386) i skonfigurować go do zarządzania skarbcem centralnym lub wieloma takimi skarbcami. Skarbce tego typu określa się jako skarbcze zarządzane (s. 385).

Węzeł magazynowania pomaga agentowi w deduplikacji kopii zapasowych przed ich przesyłaniem do skarbca zarządzanego, a także deduplikuje (s. 376) kopie zapasowe już zapisane w skarbcach. Deduplikacja zmniejsza ruch w sieci związany z tworzeniem kopii zapasowych oraz ilość miejsca zajmowanego przez kopie. Węzeł magazynowania wykonuje również operacje na archiwach, które w przeciwnym razie są wykonywane przez agenta (takie jak sprawdzanie poprawności i czyszczenie), przez co odciąża komputery zarządzane. Warto również wspomnieć, że węzeł Acronis Backup & Recovery 11 Storage Node umożliwia użycie biblioteki taśm jako skarbca centralnego do przechowywania archiwów kopii zapasowych.

Można skonfigurować wiele węzłów magazynowania, z których każdy zarządza wieloma skarbcami, a sterowanie takimi węzłami odbywa się z poziomu serwera zarządzania Acronis Backup & Recovery 11 Management Server.

Aby uzyskać szczegółowe informacje na temat węzłów magazynowania, zobacz „Węzły magazynowania” (s. 212).

11.1.2 Uprawnienia zarządzania scentralizowanego

W tej sekcji opisano uprawnienia użytkowników wymagane w celu lokalnego i zdalnego zarządzania komputerem, zarządzania komputerem zarejestrowanym na serwerze zarządzania Acronis Backup & Recovery 11 Management Server oraz uzyskania dostępu do węzła magazynowania Acronis Backup & Recovery 11 Storage Node i zarządzania nim.

Typy połączeń z komputerem zarządzanym

Istnieją dwa typy połączeń z komputerem zarządzanym: połączenie lokalne i połączenie zdalne.

Połączenie lokalne

Połączenie lokalne występuje pomiędzy konsolą zarządzania Acronis Backup & Recovery 11 Management Console na komputerze i agentem Acronis Backup & Recovery 11 Agent, znajdującym się na tym samym komputerze.

Aby ustanowić połączenie lokalne

- Na pasku narzędzi kliknij **Połącz**, a następnie wskaż **Nowe połączenie** i kliknij **Ten komputer**.

Połączenie zdalne

Połączenie zdalne występuje pomiędzy konsolą zarządzania Acronis Backup & Recovery 11 Management Console na komputerze i agentem Acronis Backup & Recovery 11 Agent, znajdującym się na innym komputerze.

Aby ustanowić połączenie zdalne, może być konieczne określenie poświadczeń logowania.

Aby ustanowić połączenie zdalne

1. Na pasku narzędzi kliknij **Połącz**, a następnie wskaż **Nowe połączenie** i kliknij **Zarządzaj komputerem zdalnym**.
2. W obszarze **Komputer** wpisz lub wybierz nazwę i adres IP komputera zdalnego, z którym połączenie ma zostać nawiązane lub kliknij **Przeglądaj**, aby wybrać komputer z listy.
3. Aby określić poświadczenia połączenia, kliknij **Opcje**, a następnie wpisz nazwę użytkownika i hasło odpowiednio w polach **Nazwa użytkownika** i **Hasło**. Jeśli w systemie Windows pole **Nazwa użytkownika** będzie puste, program użyje poświadczeń wykorzystywanych przez konsolę.
4. Aby zapisać hasło dla określonej nazwy użytkownika, zaznacz pole wyboru **Zapisz hasło**. Hasło zostanie zapisane i będzie przechowywane w bezpiecznej lokalizacji na komputerze, na którym działa konsola.

Uprawnienia do połączeń lokalnych

Windows

Połączenie lokalne na komputerze z systemem Windows może nawiązać dowolny użytkownik posiadający uprawnienia do lokalnego logowania się na tym komputerze.

Linux

Nawiązanie połączenia lokalnego na komputerze z systemem Linux i zarządzanie takim komputerem wymaga uprawnień użytkownika root.

Aby nawiązać połączenie lokalne jako użytkownik root

1. Po zalogowaniu jako użytkownik root uruchom następujące polecenie:

```
/usr/sbin/acronis_console
```

Lub następujące polecenie:

```
su -c /usr/sbin/acronis_console
```

2. Kliknij **Zarządzaj tym komputerem**.

Aby umożliwić uruchamianie konsoli użytkownikowi innemu niż root

- Jako użytkownik root dodaj do pliku **/etc/sudoers** nazwy użytkowników, którym chcesz zezwolić na uruchamianie konsoli, na przykład przy użyciu polecenia **visudo**.

Przestroga: Po wykonaniu tej procedury użytkownik inny niż root będzie mógł nie tylko uruchamiać konsolę, ale również wykonywać inne działania jako użytkownik root.

Aby nawiązać połączenie lokalne jako użytkownik inny niż root

1. Upewnij się, że użytkownik root umożliwił uruchamianie konsoli, jak opisano to w poprzedniej procedurze.
2. Uruchom następujące polecenie:

```
sudo /usr/sbin/acronis_console
```

3. Kliknij **Zarządzaj tym komputerem**.

Uprawnienia połączeń zdalnych w systemie Windows

Aby nawiązać połączenie zdalne z komputerem z systemem Windows, użytkownik musi należeć do grupy zabezpieczeń Acronis Remote Users na tym komputerze.

Po nawiązaniu połączenia zdalnego użytkownik ma prawa zarządzania na komputerze zdalnym, które opisano w sekcji Prawa użytkownika na komputerze zarządzanym (s. 33).

Uwaga: Na komputerze zdalnym z systemem Windows Vista, na którym jest włączona usługa kontroli konta użytkownika (UAC) i który nie jest częścią domeny, wyłącznie użytkownik korzystający z wbudowanego konta administratora może tworzyć kopie zapasowe danych i wykonywać operacje zarządzania. Aby obejść to ograniczenie, należy dodać komputer do domeny lub wyłączyć na nim usługę kontroli konta użytkownika (domyślnie jest ona włączona). Tę samą metodę należy zastosować na komputerach z systemami Windows Server 2008 i Windows 7.

Aby uzyskać informacje o grupach zabezpieczeń Acronis i ich członkach domyślnych, zobacz Grupy zabezpieczeń Acronis (s. 308).

Uprawnienia połączeń zdalnych w systemie Linux

Zdalne połączenia z komputerami z systemem Linux, w tym również nawiązywane przez użytkownika root, są nawiązywane zgodnie z zasadami uwierzytelniania skonfigurowanymi w module Pluggable Authentication Modules for Linux, znanym jako Linux-PAM.

Aby umożliwić działanie zasad uwierzytelniania, zalecamy zainstalowanie najnowszej wersji modułu Linux-PAM dla dystrybucji systemu Linux. Najnowszy stabilny kod źródłowy systemu Linux-PAM jest dostępny na stronie internetowej z kodem źródłowym systemu Linux-PAM.

Zdalne połączenie jako użytkownik root

Zdalne połączenia są nawiązywane przez użytkownika root zgodnie z zasadą uwierzytelniania agenta Acronis, która jest konfigurowana automatycznie podczas instalowania komponentu Acronis Backup & Recovery 11 Agent for Linux, przez utworzenie pliku `/etc/pam.d/acronisagent` o następującej zawartości:

```
##PAM-1.0
auth      required      pam_unix.so
auth      required      pam_succeed_if.so uid eq 0
account   required      pam_unix.so
```

Zdalne połączenie jako użytkownik inny niż root

Ponieważ dostęp do systemu jako użytkownik root powinien być ograniczony, użytkownik root może utworzyć zasadę uwierzytelniania, aby umożliwić zdalne zarządzanie przy użyciu poświadczeń innych niż root.

Poniżej podano dwa przykłady takich zasad.

Uwaga: W efekcie określeni użytkownicy inni niż root będą mogli zdalnie łączyć się z komputerem tak, jakby mieli uprawnienia użytkownika root. Dobrą praktyką ze względów bezpieczeństwa jest odpowiednie zabezpieczenie kont tych użytkowników przed włamaniem — na przykład przez wymóg używania na nich silnych haseł.

Przykład 1

Ta zasada uwierzytelniania używa modułu `pam_succeed_if` i działa w dystrybucjach systemu Linux z jądrem w wersji 2.6 lub nowszej. Zasadę uwierzytelniania działającą z jądrem w wersji 2.4 przedstawiono w następnym przykładzie.

Jako użytkownik root wykonaj następujące czynności:

1. Utwórz konto grupy **Acronis_Trusted**, uruchamiając następujące polecenie:

```
groupadd Acronis_Trusted
```

2. Dodaj do grupy **Acronis_Trusted** nazwy użytkowników innych niż root, którym chcesz zezwolić na zdalne łączenie się z komputerem. Aby na przykład dodać do grupy istniejącego użytkownika `user_a`, uruchom następujące polecenie:

```
usermod -G Acronis_Trusted user_a
```

3. Wyedytuj plik **/etc/pam.d/acronisagent-trusted**, jak opisano poniżej:

```
##PAM-1.0
auth      required    pam_unix.so
auth      required    pam_succeed_if.so user ingroup Acronis_Trusted
account   required    pam_unix.so
```

Przykład 2

Powyższa zasada uwierzytelniania może nie działać w dystrybucjach systemu Linux o wersji jądra 2.4 — w tym w systemie Red Hat Linux — ponieważ moduł `pam_succeed_if.so` nie jest w nich obsługiwany.

Można wtedy użyć następującej zasady uwierzytelniania.

1. Jako użytkownik root utwórz plik **/etc/pam.d/Acronis_trusted_users**
2. Dodaj do tego pliku nazwy użytkowników niebędących użytkownikami root, którym chcesz zezwolić na zarządzanie komputerem (każda nazwa w osobnym wierszu). Aby na przykład dodać użytkowników `uzytk_a`, `uzytk_b` i `uzytk_c`, dodaj do pliku następujące trzy wiersze:

```
user_a
user_b
user_c
```

W razie konieczności dodaj do pliku również użytkownika root.

3. Wyedytuj plik **/etc/pam.d/acronisagent-trusted**, jak opisano poniżej:

```
##PAM-1.0
auth      required    pam_unix.so
auth      required    pam_listfile.so item=user sense=allow
file=/etc/pam.d/Acronis_trusted_users onerr=fail
account   required    pam_unix.so
```

Grupy zabezpieczeń Acronis

Na komputerze z systemem Windows grupy zabezpieczeń Acronis określają, kto może zdalnie zarządzać komputerem i działać jako administrator serwera Acronis Backup & Recovery 11 Management Server.

Grupy te są tworzone podczas instalowania agentów Acronis Backup & Recovery 11 lub serwera Acronis Backup & Recovery 11 Management Server. Można wówczas określić użytkowników należących do poszczególnych grup.

Agenty Acronis Backup & Recovery 11

Podczas instalowania na komputerze agenta Acronis Backup & Recovery 11 Agent for Windows program tworzy (lub aktualizuje) grupę **Acronis Remote Users**.

Użytkownik należący do tej grupy może zarządzać zdalnie komputerem przy użyciu konsoli Acronis Backup & Recovery 11 Management Console, zgodnie z uprawnieniami do zarządzania opisanymi w sekcji Przywileje użytkowników na zarządzanych komputerach (s. 33).

Domyślnie do tej grupy należą wszyscy członkowie grupy Administratorzy.

Serwer Acronis Backup & Recovery 11 Management Server

Podczas instalowania na komputerze serwera Acronis Backup & Recovery 11 Management Server program tworzy (lub aktualizuje) dwie grupy:

Acronis Centralized Admins

Użytkownik należący do tej grupy jest administratorem serwera zarządzania. Administratorzy serwera zarządzania mogą łączyć się z serwerem zarządzania przy użyciu konsoli Acronis Backup & Recovery 11 Management Console. Mają oni takie same uprawnienia do zarządzania na zarejestrowanych komputerach, jak użytkownicy z uprawnieniami administracyjnymi na tych komputerach — niezależnie od zawartości grup zabezpieczeń Acronis.

Aby nawiązać *zdalne* połączenie z serwerem zarządzania, administrator serwera zarządzania musi również należeć do grupy zdalnych użytkowników Acronis Remote Users.

Żaden użytkownik, nawet należący do grupy Administratorzy, nie może być administratorem serwera zarządzania, jeśli nie należy do grupy administratorów centralnych Acronis Centralized Admins.

Domyślnie do tej grupy należą wszyscy członkowie grupy Administratorzy.

Acronis Remote Users

Użytkownik należący do tej grupy może nawiązywać zdalne połączenie z serwerem zarządzania przy użyciu konsoli Acronis Backup & Recovery 11 Management Console, pod warunkiem, że należy również do grupy administratorów centralnych Acronis Centralized Admins.

Domyślnie do tej grupy należą wszyscy członkowie grupy Administratorzy.

Informacje na temat kontrolera domeny

Jeśli komputer jest kontrolerem domeny Active Directory, nazwy i domyślna zawartość grup zabezpieczeń Acronis są inne:

- Grupy zdalnych użytkowników **Acronis Remote Users** i administratorów centralnych **Acronis Centralized Admins** noszą odpowiednio nazwy **DCNAME \$ Acronis Remote Users** i **DCNAME \$ Acronis Centralized Admins**. **DCNAME** oznacza nazwę NetBIOS kontrolera domeny. Po obu stronach każdego znaku dolara występują pojedyncze spacje.
- Zamiast bezpośredniego uwzględnienia nazw wszystkich członków grupy Administratorzy dołączona jest cała grupa Administratorzy.

Wskazówka: Aby zapewnić odpowiednie nazwy grup, należy zainstalować komponenty Acronis na kontrolerze domeny po jego skonfigurowaniu. Jeśli komponenty będą zainstalowane przed skonfigurowaniem kontrolera domeny, należy ręcznie utworzyć grupy zdalnych użytkowników **DCNAME \$ Acronis Remote users** i administratorów centralnych **DCNAME \$ Acronis Centralized Admins**, a następnie dodać do nich członków grup **Acronis Remote Users** i **Acronis Centralized Admins**.

Prawa administratora serwera zarządzania

Zwykle administrator serwera zarządzania Acronis Backup & Recovery 11 Management Server działa na komputerze zarejestrowanym w imieniu usługi komputera zarządzanego Acronis Managed Machine Service (znanej również jako usługa Acronis) uruchomionej na tym komputerze i z jej uprawnieniami.

Ewentualnie, tworząc scentralizowany plan tworzenia kopii zapasowych, administrator serwera zarządzania może wprost określić konto użytkownika, w ramach którego wykonywany będzie scentralizowany plan tworzenia kopii zapasowych na komputerach zarejestrowanych. W takim przypadku dane konto użytkownika musi istnieć na wszystkich komputerach, na których zostanie wdrożony scentralizowany plan tworzenia kopii zapasowych. Nie zawsze jest to metoda efektywna.

Administratorem serwera zarządzania musi być użytkownik będący członkiem grupy Acronis Centralized Admins (Administratorów centralnych) na komputerze, na którym jest zainstalowany serwer zarządzania.

Prawa do usług Acronis

Komponenty Acronis Backup & Recovery 11 Agent for Windows, Acronis Backup & Recovery 11 Agent for VMware vSphere ESX(i) (Windows), Acronis Backup & Recovery 11 Management Server i Acronis Backup & Recovery 11 Storage Node działają jako usługi. Podczas instalacji dowolnego z tych komponentów należy określić konto, na którym będzie uruchamiana jego usługa.

Dla każdej usługi można utworzyć specjalne konto użytkownika (zalecane w większości przypadków) albo określić istniejące konto użytkownika lokalnego lub użytkownika domeny, na przykład: **.\UżytkownikLokalny** lub **NazwaDomeny\UżytkownikDomeny**.

Nowe konta

W przypadku decyzji o utworzeniu specjalnych kont użytkowników dla usług program utworzy następujące konta użytkowników:

- Dla usługi komponentów Acronis Backup & Recovery 11 Agent for Windows i Acronis Backup & Recovery 11 Agent for VMware vSphere ESX(i) (Windows): **Acronis Agent User**
- Dla usługi serwera Acronis Backup & Recovery 11 Management Server: **AMS User**
- Dla usługi węzła Acronis Backup & Recovery 11 Storage Node: **ASN User**

Nowo utworzone konta otrzymają następujące uprawnienia:

- Do wszystkich trzech kont program przypisze prawo użytkownika **Logowanie jako usługa**.
- Konto użytkownika Acronis Agent User otrzyma uprawnienia **Dostosuj przydziały pamięci dla procesów, Zamień token na poziomie procesu i Modyfikuj wartości środowiskowe oprogramowania układowego**.
- Konta użytkowników Acronis Agent User i ASN User zostaną włączone do grup **Operatorzy kopii zapasowych i Administratorzy**.
- Konto Użytkownik AMS User jest dołączone do grupy **Acronis Centralized Admins**.

Istniejące konta

Program instalacyjny przypisze powyższe uprawnienia użytkownika do dowolnego istniejącego konta, które zostało określone dla wybranej usługi.

W przypadku decyzji o określeniu dla usługi agenta istniejącego konta użytkownika przed kontynuowaniem instalacji należy sprawdzić, czy dane konto należy do grupy **Operatorzy kopii zapasowych**. W przypadku wersji zaawansowanych konto powinno należeć do grupy **Administratorzy**. W przeciwnym razie Dostawca kopiowania w tle oprogramowania firmy Microsoft może nie wykonywać migawek podczas tworzenia scentralizowanych kopii zapasowych.

W przypadku decyzji o określeniu dla usługi węzła magazynu istniejącego konta użytkownika przed kontynuowaniem instalacji należy sprawdzić, czy dane konto należy do grupy **Administratorzy**. W przeciwnym razie usługa może nie mieć dostępu do niektórych zasobów systemu Windows.

Jeśli dla usługi serwera zarządzania określisz istniejące konto użytkownika, program automatycznie doda to konto do grupy **Acronis Centralized Admins**.

Podczas instalowania agenta **w węźle klastra awaryjnego**, takiego jak węzeł klastra Hyper-V, określ dla usługi agenta istniejące konto użytkownika domeny. Konto musi mieć uprawnienia administracyjne na każdym z węzłów klastra. To konto umożliwia agentowi dostęp do zasobów

klastra w dowolnym węźle. Można również wybrać opcję utworzenia nowego konta dla agenta. W takim przypadku podczas tworzenia scentralizowanych planów tworzenia kopii zapasowych lub zadań odzyskiwania będzie konieczne określenie poświadczeń konta domeny z wymaganymi uprawnieniami.

Wskazówki dotyczące dalszego użycia

- Jeśli komputer należy do domeny Active Directory, upewnij się, że zasady zabezpieczeń domeny nie uniemożliwiają kontom opisanym w tej sekcji (istniejącym lub nowo utworzonym) posiadania wymienionych wyżej praw użytkownika.

Po instalacji nie należy określać innego konta użytkownika dla usługi komponentu. W przeciwnym przypadku komponent może przestać działać.

Nowo utworzone konta użytkowników mają również dostęp do klucza rejestru HKEY_LOCAL_MACHINE\SOFTWARE\Acronis (określanego jako klucz rejestru Acronis) z następującymi prawami: **Zapytanie o wartość**, **Ustawianie wartości**, **Tworzenie podklucza**, **Wyliczanie podkluczy**, **Powiadamanie**, **Usuwanie** oraz **Kontrola odczytu**.

Dodatkowo dwie usługi Acronis są uruchamiane na koncie systemowym:

- Usługa **Acronis Scheduler2 Service** umożliwia tworzenie harmonogramów zadań komponentów Acronis. Jest uruchamiana na lokalnym koncie systemowym i nie można jej uruchamiać na żadnym innym koncie.
- Usługa **Acronis Remote Agent Service** umożliwia łączność między komponentami Acronis. Jest uruchamiana na koncie usługi sieciowej i nie można jej uruchamiać na żadnym innym koncie.

11.1.3 Komunikacja między komponentami programu Acronis Backup & Recovery 11

W tej sekcji opisano sposób komunikowania się ze sobą komponentów programu Acronis Backup & Recovery 11 przy użyciu bezpiecznego uwierzytelniania i szyfrowania.

Ta sekcja zawiera także informacje na temat konfigurowania ustawień komunikacji, wybierania portu sieciowego do komunikacji i zarządzania certyfikatami zabezpieczeń.

Bezpieczna komunikacja

Program Acronis Backup & Recovery 11 zapewnia ochronę danych przesyłanych pomiędzy jego komponentami w sieci lokalnej i sieci granicznej (zwanej również strefą zdemilitaryzowaną, DMZ).

Istnieją dwa mechanizmy, które zapewniają bezpieczną komunikację pomiędzy komponentami programu Acronis Backup & Recovery 11:

- **Bezpieczne uwierzytelnianie** zapewnia bezpieczny transfer certyfikatów potrzebnych do ustanowienia połączenia poprzez wykorzystanie protokołu SSL.
- **Komunikacja zaszyfrowana** umożliwia bezpieczny transfer informacji pomiędzy dowolnymi dwoma komponentami — na przykład agentem Acronis Backup & Recovery 11 Agent i węzłem magazynowania Acronis Backup & Recovery 11 Storage Node — poprzez szyfrowanie przesyłanych danych.

Instrukcje dotyczące konfiguracji bezpiecznego uwierzytelniania i ustawień szyfrowania danych znajdują się w sekcji Konfiguracja opcji komunikacji (s. 312).

Instrukcje dotyczące zarządzania certyfikatami SSL wykorzystywanymi do bezpiecznego uwierzytelniania znajdują się w sekcji Certyfikaty SSL (s. 313).

Uwaga: Łączność pomiędzy komponentami wcześniejszych produktów Acronis, w tym z rodziny Acronis True Image Echo a komponentami programu Acronis Backup & Recovery 11 jest niemożliwa, niezależnie od ustawień bezpiecznego uwierzytelniania i szyfrowania danych.

Aplikacje klienckie i serwerowe

W procesie bezpiecznej komunikacji udział biorą dwie strony:

- **Aplikacja kliencka** (klient) to aplikacja, która próbuje nawiązać połączenie.
- **Aplikacja serwerowa** (serwer) to aplikacja, z którą klient próbuje nawiązać połączenie.

Na przykład jeśli konsola Acronis Backup & Recovery 11 Management Console łączy się z agentem Acronis Backup & Recovery 11 na komputerze zdalnym, konsola jest klientem, a agent jest serwerem.

Komponent Acronis może służyć jako aplikacja kliencka, aplikacja serwerowa lub jako oba typy aplikacji, zgodnie z poniższą tabelą.

Nazwa komponentu	Może być klientem	Może być serwerem
Acronis Backup & Recovery 11 Management Console	Tak	Nie
Acronis Backup & Recovery 11 Agent	Tak	Tak
Acronis Backup & Recovery 11 Management Server	Tak	Tak
Acronis Backup & Recovery 11 Storage Node	Tak	Tak
Acronis PXE Server	Nie	Tak
Acronis Backup & Recovery 11 Bootable Agent	Tak	Tak

Konfigurowanie ustawień komunikacji

Ustawienia komunikacji, na przykład szyfrowanie przesyłanych danych, dotyczące komponentów programu Acronis Backup & Recovery 11 zainstalowanych na jednym lub większej liczbie komputerów, można skonfigurować za pomocą szablonu administracyjnego Acronis Administrative Template. Aby uzyskać informacje na temat sposobu ładowania tego szablonu, zobacz Jak załadować szablon Acronis Administrative Template (s. 360).

Szablon administracyjny zastosowany do jednego komputera definiuje ustawienia komunikacji dla wszystkich komponentów na tym komputerze. Szablon zastosowany do domeny lub jednostki organizacyjnej definiuje ustawienia komunikacji dla wszystkich komponentów na komputerach w tej domenie lub jednostce organizacyjnej.

Aby skonfigurować ustawienia komunikacji

1. Kliknij **Start**, kliknij **Uruchom** i wpisz **gpedit.msc**.
2. W konsoli **Zasady grupy** rozwiń kolejno węzły **Konfiguracja komputera** i **Szablony administracyjne**, a następnie kliknij **Acronis**.
3. W panelu **Acronis** po prawej stronie kliknij dwukrotnie opcję komunikacji, którą chcesz skonfigurować. Szablon administracyjny zawiera następujące opcje (s. 371):
 - **Porty zdalnego agenta**
 - **Opcje szyfrowania klienta**
 - **Opcje szyfrowania serwera**

4. Aby nowe ustawienia komunikacji zaczęły obowiązywać, uruchom ponownie wszystkie działające komponenty Acronis, najlepiej uruchamiając ponownie system Windows. Jeśli ponowne uruchomienie nie jest możliwe, wykonaj następujące czynności:
 - Jeśli konsola Acronis Backup & Recovery 11 Management Console jest uruchomiona, zamknij ją i uruchom ponownie.
 - Jeśli uruchomione są inne komponenty Acronis, takie jak Acronis Backup & Recovery 11 Agent for Windows lub Acronis Backup & Recovery 11 Management Server, uruchom ponownie odpowiednie usługi w przystawce **Usługi** w systemie Windows.

Konfiguracja portu sieciowego

Domyślnie komponenty programu Acronis Backup & Recovery 11 korzystają z portu komunikacji sieciowej 9876/TCP. Serwer nasłuchuje ten port pod kątem połączeń przychodzących. Klient Acronis również wykorzystuje ten port jako domyślny. Jeśli użytkownik korzysta z zapory ogniowej innej niż Zapora systemu Windows, może zostać poproszony podczas instalacji komponentu o potwierdzenie otwarcia portu lub o ręczne jego otwarcie.

W dowolnym momencie po instalacji porty można zmienić według preferowanych wartości lub dla celów bezpieczeństwa. Ta operacja wymaga ponownego uruchomienia agenta Acronis Remote Agent (w systemie Windows) lub usługi Acronis_agent (w systemie Linux).

Po zmianie portu po stronie serwera połącz się z serwerem używając notacji URL <IP_serwera>:<port> lub <nazwa_hosta_serwera>:<port>.

Uwaga: Jeśli użytkownik korzysta z translatora adresów sieciowych (NAT), port można skonfigurować również za pomocą ustawienia mapowania portu.

Konfiguracja portu w systemie operacyjnym

Windows

Aby umożliwić zmianę numerów portów, należy załadować i skonfigurować Administrative Template firmy Acronis zgodnie z opisem w sekcji Konfiguracja ustawień komunikacji (s. 312), w części „Porty agenta zdalnego”.

Linux

Określ port w pliku /etc/Acronis/Policies/Agent.config. Uruchom ponownie Acronis_agent daemon.

Konfiguracja portu w środowisku startowym

Tworząc nośnik startowy Acronis, można wstępnie skonfigurować port sieciowy, z którego korzystał będzie agent startowy Acronis Backup & Recovery 11 Bootable Agent. Dostępne są następujące opcje:

- Port domyślny (9876)
- Aktualnie wykorzystywany port
- Nowy port (wprowadź numer portu)

Jeśli nie nastąpiła wstępna konfiguracja portu, agent użyje numeru portu domyślnego.

Certyfikaty SSL

W celu bezpiecznego uwierzytelniania komponenty programu Acronis Backup & Recovery 11 używają certyfikatów Secure Sockets Layer (SSL).

Istnieją dwa rodzaje certyfikatów SSL komponentów:

- **Certyfikaty z podpisem własnym**, na przykład certyfikaty generowane automatycznie podczas instalacji komponentu Acronis
- **Certyfikaty bez podpisu własnego**, na przykład certyfikaty wydawane przez niezależne urzędy certyfikacji, takie jak publiczny urząd certyfikacji VeriSign® lub Thawte™, lub przez urząd certyfikacji przedsiębiorstwa użytkownika

Ścieżka certyfikatu

Wszystkie komponenty Acronis zainstalowane na komputerze i spełniające funkcje serwera aplikacji korzystają z certyfikatu SSL zwanego certyfikatem serwera.

W systemie Windows ścieżka certyfikatu i nazwa pliku certyfikatu serwera określone są w kluczu rejestru `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Encryption\Server`. Domyślna ścieżka to:

- W 32-bitowych wersjach systemu Windows: `%CommonProgramFiles%\Acronis\Agent`
- W 64-bitowych wersjach systemu Windows: `%CommonProgramFiles(x86)%\AcronisAgent`

W przypadku certyfikatów z podpisem własnym odcisk certyfikatu (znany również skrótem) umożliwia przyszłą identyfikację hosta: jeśli klient uprzednio połączył się z serwerem za pomocą certyfikatu z podpisem własnym i próbuje ponownie uzyskać połączenie, serwer sprawdza, czy odcisk certyfikatu jest taki sam jak użyty ostatnim razem.

Certyfikaty z podpisem własnym

Jeśli na komputerach z systemem Windows lokalizacja certyfikatów nie zawiera certyfikatu serwera, program automatycznie wygeneruje certyfikat serwera z podpisem własnym, który zostanie zainstalowany podczas instalacji dowolnego komponentu Acronis z wyjątkiem konsoli Acronis Backup & Recovery 11 Management Console.

Jeśli po wygenerowaniu certyfikatu z podpisem własnym nazwa danego komputera zostanie zmieniona, certyfikatu nie będzie można użyć i należy wygenerować nowy.

Aby wygenerować nowy certyfikat z podpisem własnym

1. Zaloguj się jako członek grupy Administratorzy.
2. W menu **Start** kliknij **Uruchom**, a następnie wpisz: **cmd**
3. Uruchom następujące polecenie (zwracając uwagę na cudzysłów):
 - W przypadku używania 32-bitowej wersji systemu Windows:

```
"%CommonProgramFiles%\Acronis\Utils\acroniscert" --reinstall
```
 - W przypadku używania 64-bitowej wersji systemu Windows:

```
"%CommonProgramFiles(x86)%\Acronis\Utils\acroniscert" --reinstall
```
4. Uruchom ponownie system Windows lub aktywne usługi Acronis.

Certyfikaty bez podpisu własnego

Zamiast certyfikatów z podpisem własnym można używać certyfikatów wystawionych przez zaufanych niezależnych wydawców albo utworzonych przez urząd certyfikacji własnego przedsiębiorstwa. Służy do tego narzędzie Acronis Certificate Command-line Utility.

Aby zainstalować certyfikat niezależnego podmiotu

1. Kliknij **Start**, następnie **Uruchom**, a następnie wpisz: **certmgr.msc**
2. W konsoli **Certyfikaty** kliknij dwukrotnie nazwę certyfikatu do zainstalowania.

3. Na karcie **Szczegóły** na liście pól kliknij **Odcisk palca**.
4. Zaznacz i skopiuj wartość pola, zwaną odciskiem certyfikatu — na przykład ciąg **20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85**
5. W menu **Start** kliknij **Uruchom**, a następnie wpisz poniższy tekst w polu **Otwórz** (jeśli używasz 64-bitowej wersji systemu Windows, zastąp ciąg **%CommonProgramFiles%** ciągiem **%CommonProgramFiles(x86)%**):

```
"%CommonProgramFiles%\Acronis\Utils\acroniscert.exe" --install  
"20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85"
```

(Zwróć uwagę na cudzysłowy. Zastąp ten przykładowy odcisk wartością skopiowaną z certyfikatu).

11.2 Tworzenie scentralizowanego planu tworzenia kopii zapasowych

Scentralizowany plan tworzenia kopii zapasowych można zastosować zarówno na komputerach z systemem Windows, jak i z systemem Linux.

Czynności wymagane do utworzenia scentralizowanego planu tworzenia kopii zapasowych przypominają etapy procedury tworzenia planu tworzenia kopii zapasowych (s. 48) z wyjątkiem następujących działań:

- Podczas wybierania danych do uwzględnienia w kopii zapasowej można zarówno bezpośrednio wybierać elementy na zarejestrowanych komputerach, jak i skorzystać z reguł wyboru. Aby uzyskać więcej informacji, zobacz „Wybieranie danych do uwzględnienia w kopii zapasowej” (s. 315).
- Określając miejsce przechowywania archiwów komputerów, można wybrać opcję przechowywania:
 - archiwów wszystkich komputerów w jednej lokalizacji;
 - archiwum każdego komputera w określonym folderze na komputerze;
 - archiwum każdego komputera w jego strefie Acronis Secure Zone.Aby uzyskać więcej informacji, zobacz „Wybór lokalizacji” (s. 322).
- Podczas konfigurowania harmonogramu dziennego, tygodniowego lub miesięcznego dostępne są zaawansowane ustawienia harmonogramu. Aby uzyskać więcej informacji, zobacz „Zaawansowane ustawienia harmonogramu” (s. 85).

11.2.1 Wybieranie danych do uwzględnienia w kopii zapasowej

Aby wybrać dane uwzględniane w kopii zapasowej

1. W sekcji **Dane uwzględniane w kopii zapasowej** wybierz typ danych, które chcesz uwzględnić w kopii zapasowej. Lista dostępnych typów danych zależy od agentów uruchomionych na komputerze:

Komputery/dyski/woluminy

Wybór tej opcji umożliwia utworzenie kopii zapasowej:

- całych komputerów fizycznych, ich dysków lub woluminów, jeśli został zainstalowany komponent Acronis Backup & Recovery 11 Agent for Windows lub Acronis Backup & Recovery 11 Agent for Linux.

Aby tworzyć kopie zapasowe tych danych, musisz mieć uprawnienia administratora lub operatora kopii zapasowych.

Dzięki utworzeniu kopii zapasowej na poziomie dysku można odzyskać cały system w razie poważnego uszkodzenia danych lub awarii sprzętu. Procedura tworzenia kopii zapasowej jest szybsza niż operacja kopiowania plików, a może znacząco przyspieszyć proces tworzenia kopii zapasowej w przypadku dużych woluminów danych.

- całych maszyn wirtualnych znajdujących się na serwerze wirtualizacji, ich dysków lub woluminów, jeśli został zainstalowany komponent Acronis Backup & Recovery 11 Agent for ESX(i) lub Acronis Backup & Recovery 11 Hyper-V.

Utworzenie kopii zapasowej całej maszyny wirtualnej, jej dysków lub woluminów powoduje utworzenie standardowej kopii zapasowej dysku (s. 381). Dodatkowo w kopii zapasowej jest przechowywana konfiguracja maszyny wirtualnej. Będzie ona domyślnie sugerowana podczas odzyskiwania zawartości kopii zapasowej na nową maszynę wirtualną. Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych maszyn wirtualnych, zobacz „Tworzenie kopii zapasowych maszyn wirtualnych”.

Foldery/pliki

Opcja dostępna, jeśli zainstalowano komponent Acronis Backup & Recovery 11 Agent for Windows lub Acronis Backup & Recovery 11 Agent for Linux.

Wybór tej opcji umożliwia utworzenie kopii zapasowej określonych plików i folderów.

Kopia zapasowa na poziomie pliku nie wystarcza do odzyskania systemu operacyjnego. Wybierz opcję tworzenia kopii zapasowej plików, jeśli planujesz zabezpieczenie tylko określonych danych (na przykład bieżącego projektu). Rozmiar archiwum będzie mniejszy, a więc w magazynie zostanie więcej miejsca.

Aby móc odzyskać system operacyjny z wszystkimi ustawieniami i aplikacjami, należy utworzyć kopię zapasową dysku.

2. Wybierz sposób wybierania elementów:

- **Wybierz elementy bezpośrednio** (domyślnie) — zalecany w przypadkach tworzenia na wielu komputerach kopii zapasowych różnych elementów danych. Na przykład: *FolderA* na komputerze *Komputer1*, *FolderB* na komputerze *Komputer2*, *FolderC* na komputerze *Komputer3* itp.

Zaznaczenie pola wyboru obok komputera oznacza uwzględnienie w kopii zapasowej wszystkich jego dysków. Aby wybrać pojedyncze dyski lub woluminy, rozwiń komputer i zaznacz pola wyboru obok odpowiednich dysków lub woluminów.

Uwagi dotyczące komputerów fizycznych, ich dysków i woluminów

- Jeśli system operacyjny i jego program ładujący znajdują się na różnych woluminach, w kopii zapasowej należy zawsze uwzględnić oba woluminy. Woluminy muszą być również odzyskiwane wspólnie, gdyż w przeciwnym razie istnieje duże ryzyko, że system operacyjny nie uruchomi się.
- Uwagi dla użytkowników systemu Linux: woluminy logiczne i urządzenia MD są widoczne w sekcji **Woluminy dynamiczne**. Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych takich woluminów i urządzeń, zobacz „Tworzenie kopii zapasowych oraz odzyskiwanie woluminów logicznych i urządzeń MD (Linux)” (s. 39).
- Uwaga dla użytkowników systemu Linux: Zaleca się odmontowanie wszystkich woluminów zawierających systemy plików bez funkcji księgowania — na przykład system ext2 — przed utworzeniem ich kopii zapasowej. W przeciwnym przypadku po odzyskaniu woluminy te mogą zawierać uszkodzone pliki, a odzyskiwanie ze zmianą rozmiaru może zakończyć się niepowodzeniem.

Uwagi dotyczące maszyn wirtualnych, ich dysków i woluminów

- Tworzenie kopii zapasowych całych maszyn wirtualnych jest przydatne, gdy istnieje duża liczba małych (pod względem rozmiarów dysków wirtualnych) serwerów starszego typu,

na przykład powstałych w związku z konsolidacją obciążenia. Dla każdej maszyny tworzone jest osobne archiwum.

- Tworzenie kopii zapasowych pojedynczych dysków lub woluminów maszyny wirtualnej jest przydatne, gdy system operacyjny i aplikacje, na przykład serwer bazy danych, działają na dysku wirtualnym, ale dane, na przykład baza danych, są przechowywane na dysku fizycznym o dużej pojemności dodanym do tej samej maszyny. Można użyć różnych strategii tworzenia kopii zapasowych dysków wirtualnych i pamięci fizycznej.

Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych maszyn wirtualnych, zobacz „Tworzenie kopii zapasowych maszyn wirtualnych”.

- **Wybierz przy użyciu reguł zasad** — opcja najodpowiedniejsza w przypadkach tworzenia na wielu komputerach kopii zapasowych tych samych elementów danych. Dotyczy to na przykład tworzenia kopii zapasowej woluminu systemowego na każdym zaznaczonym komputerze.

Więcej informacji znajduje się w następujących sekcjach:

Reguły wyboru plików i folderów (s. 317)

Reguły wyboru woluminów (s. 319)

3. Po określeniu danych uwzględnianych w kopii zapasowej kliknij **OK**.

11.2.2 Reguły wyboru plików i folderów

Zdefiniuj reguły wyboru plików. Na podstawie tych reguł będą tworzone kopie zapasowe plików i/lub folderów na komputerach uwzględnionych w scentralizowanym planie tworzenia kopii zapasowych.

Aby zdefiniować reguły wyboru plików

1. Wybierz regułę z listy rozwijanej (lub wpisz ją ręcznie) i kliknij **Dodaj regułę**. Program zapamiętuje reguły wpisane ręcznie, dlatego następnym razem po otwarciu okna reguły te będą dostępne na liście razem z regułami domyślnymi.
2. W prawej części okna zaznacz pola wyboru obok komputerów lub grup, do których chcesz zastosować reguły.

Windows

Pełna ścieżka

Wskaż foldery i pliki do utworzenia kopii zapasowej. Jeśli określisz dokładną ścieżkę do pliku lub folderu, plan spowoduje utworzenie kopii zapasowej tego elementu na wszystkich komputerach, na których zostanie znaleziona dokładnie taka ścieżka.

Elementy uwzględniane	W kolumnie Pliki i foldery wpisz lub wybierz:
Plik Text.doc w folderze D:\Work	D:\Work\Text.doc
Folder C:\Windows	C:\Windows

Zmienne środowiskowe

Niektóre zmienne środowiskowe wskazują foldery systemu Windows. Korzystanie z takich zmiennych zamiast pełnych ścieżek do plików i folderów gwarantuje, że kopia zapasowa właściwych folderów systemu Windows zostanie utworzona niezależnie od lokalizacji systemu Windows na konkretnym komputerze.

Elementy uwzględniane	W kolumnie Pliki i foldery wpisz lub wybierz	Komentarze
Folder Program Files	%PROGRAMFILES%	Wskazuje folder Program Files (na przykład C:\Program Files)
Folder systemu Windows	%WINDIR%	Wskazuje folder, w którym znajdują się pliki systemu Windows (na przykład C:\Windows)
Typowe dane dotyczące wszystkich profili użytkowników	%ALLUSERSPROFILE%	Wskazuje folder, w którym znajdują się wspólne dane wszystkich profili użytkowników (zwykle C:\Documents and Settings\All Users w systemie Windows XP i C:\ProgramData w systemie Windows Vista)

Można korzystać z innych zmiennych środowiskowych lub łączyć zmienne środowiskowe i tekst. Aby na przykład odwołać się do folderu Acronis znajdującego się na komputerach w folderze Program Files, wpisz: **%PROGRAMFILES%\Acronis**

Szablony

Szablony przypominają zmienne środowiskowe, ale są już wstępnie dostosowane.

Elementy uwzględniane	W kolumnie Pliki i foldery wpisz lub wybierz:	Komentarze
Wszystkie pliki we wszystkich woluminach na komputerze	[Wszystkie pliki]	Wskazuje wszystkie pliki we wszystkich woluminach na komputerze.
Wszystkie profile użytkowników istniejące na komputerze	[Wszystkie foldery profilów]	Wskazuje folder, w którym znajdują się wszystkie profile użytkowników (zwykle C:\Documents and Settings w systemie Windows XP i C:\Users w systemie Windows Vista).

Linux

Elementy uwzględniane	W kolumnie Pliki i foldery wpisz lub wybierz:
Plik tekstowy file.txt w woluminie /dev/hda3 zamontowanym na /home/usr/docs	/dev/hda3/file.txt lub /home/usr/docs/file.txt
Katalog główny typowych użytkowników	/home
Katalog główny użytkownika root	/root
Katalog dla wszystkich programów użytkowników	/usr
Katalog plików konfiguracyjnych systemu	/etc

11.2.3 Reguły wyboru woluminów

Zdefiniuj reguły wyboru woluminów. Na podstawie tych reguł będą tworzone kopie zapasowe woluminów na komputerach, które mają być uwzględnione w scentralizowanym planie tworzenia kopii zapasowych.

Aby zdefiniować reguły wyboru woluminów

1. Wybierz regułę z listy rozwijanej (lub wpisz ją ręcznie) i kliknij **Dodaj regułę**. Program zapamiętuje reguły wpisane ręcznie, dlatego następnym razem po otwarciu okna reguły te będą dostępne na liście razem z regułami domyślnymi.
2. W prawej części okna zaznacz pola wyboru obok komputerów lub grup, do których chcesz zastosować reguły.

W poniższej tabeli znajduje się objaśnienie reguł wstępnie zdefiniowanych, które można wybrać na liście. W nazwach szablonów jest uwzględniana wielkość liter.

Elementy uwzględniane	W oknie reguł wyboru:	Komentarze
Woluminy systemów Windows i Linux		
Wszystkie woluminy	Wpisz lub wybierz: [Wszystkie woluminy]	Dotyczy wszystkich woluminów na komputerach z systemem Windows i wszystkich zamontowanych woluminów na komputerach z systemem Linux.
Woluminy systemu Windows		
Wolumin C:	Wpisz C:\ lub wybierz tę pozycję z listy	
Wolumin systemowy	Wpisz lub wybierz: [SYSTEM]	Wolumin systemowy zawiera pliki specyficzne dla sprzętu, takie jak Ntldr, Boot.ini i Ntdetect.com, które są potrzebne do uruchomienia systemu Windows. Istnieje tylko jeden wolumin systemowy, nawet jeśli na komputerze jest zainstalowanych wiele systemów operacyjnych Windows. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Windows” poniżej.
Wolumin startowy	Wpisz lub wybierz: [BOOT]	Dotyczy woluminu startowego na komputerze zarejestrowanym. Wolumin startowy zawiera folder systemu operacyjnego Windows i pliki pomocnicze tego systemu (zwykle znajdują się one w folderze Windows\System32). Może on być woluminem systemowym, ale nie musi. Jeśli na komputerze jest zainstalowanych wiele systemów operacyjnych, jest to wolumin startowy systemu operacyjnego, w którym jest zainstalowany agent. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Windows” poniżej.
Wszystkie woluminy stałe	Wpisz lub wybierz: [Woluminy stałe]	Dotyczy wszystkich woluminów innych niż nośniki wymienne. Woluminy stałe znajdują się na urządzeniach SCSI, ATAPI, ATA, SSA, SAS i SATA oraz macierzach RAID.

Pierwszy dysk	Wpisz lub wybierz: [Dysk 1]	Odpowiada pierwszemu dysкови zarejestrowanego komputera i obejmuje wszystkie woluminy na tym dysku.
Woluminy systemu Linux		
Pierwsza partycja na pierwszym dysku twardym IDE komputera z systemem Linux	Wpisz lub wybierz: /dev/hda1	hda1 to standardowa nazwa urządzenia oznaczająca pierwszą partycję na pierwszym dysku twardym IDE. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Linux” poniżej.
Pierwsza partycja na pierwszym dysku twardym SCSI komputera z systemem Linux	Wpisz lub wybierz: /dev/sda1	sda1 to standardowa nazwa urządzenia oznaczająca pierwszą partycję na pierwszym dysku twardym SCSI. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Linux” poniżej.
Pierwsza partycja na pierwszym programowym dysku twardym RAID komputera z systemem Linux	Wpisz lub wybierz: /dev/md1	md1 to standardowa nazwa urządzenia oznaczająca pierwszą partycję na pierwszym programowym dysku RAID. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Linux” poniżej.

Uwaga dotycząca komputerów z systemem Windows

Systemy operacyjne Windows starsze niż Windows 7 i Windows Server 2008 R2 zapisują pliki systemowe i program ładujący na tym samym woluminie, chyba że podczas instalacji został określony inny wolumin. Jeśli pliki systemu Windows i program ładujący znajdują się na tym samym woluminie, wybranie opcji **[SYSTEM]** lub **[BOOT]** wystarcza do utworzenia kopii zapasowej całego systemu operacyjnego. W przeciwnym razie należy wybrać obie opcje: **[SYSTEM]** i **[BOOT]**.

Systemy operacyjne Windows 7, Windows Server 2008 R2 oraz nowsze tworzą specjalny wolumin systemowy o nazwie **System Reserved**. W razie wybrania opcji **[SYSTEM]** program utworzy kopię zapasową tylko tego specjalnego woluminu. W przypadku tworzenia kopii zapasowych komputerów z tymi systemami operacyjnymi należy zawsze wybierać obie opcje: **[SYSTEM]** i **[BOOT]**.

Ponieważ scentralizowane plany tworzenia kopii zapasowych obejmują zwykle wiele komputerów z różnymi systemami operacyjnymi, firma Acronis zaleca wybieranie zawsze obu woluminów (systemowego i startowego) w celu utworzenia kopii zapasowej. Zapewnia to integralność każdego z systemów operacyjnych.

Uwaga dotycząca komputerów z systemem Linux

W jednym scentralizowanym planie tworzenia kopii zapasowych można uwzględnić zarówno woluminy (partycje) systemu Windows, jak i systemu Linux.

Na przykład można skonfigurować scentralizowany plan tworzenia kopii zapasowych woluminu **C:** na komputerach z systemem Windows oraz partycji **/dev/hda1** na komputerach z systemem Linux.

W systemie Linux, w odróżnieniu od systemu Windows, nie ma wyraźnej różnicy między woluminem (partycją) a folderem (katalogiem). W systemie Linux istnieje partycja główna (oznaczona jako /), do której są podłączone (zamontowane) elementy różnego typu, w tym dyski twarde, katalogi i urządzenia systemowe. Tworzą one drzewo przypominające strukturę plików i folderów systemu Windows.

Załóżmy na przykład, że na komputerze z systemem Linux znajduje się dysk twardy podzielony na trzy woluminy, czyli partycje: pierwszą, drugą i trzecią. Partycje te są dostępne w drzewie odpowiednio jako **/dev/hda1**, **/dev/hda2** i **/dev/hda3**. Aby utworzyć kopię zapasową trzeciej partycji, w oknie dialogowym **Dane uwzględniane w kopii zapasowej** należy wpisać regułę **/dev/hda3**.

Ponadto partycję systemu Linux można zamontować w dowolnym miejscu drzewa. Na przykład partycja `/dev/hda3` może być zamontowana jako „podkatalog” w drzewie. Drzewem może być na przykład katalog `/home/usr/docs`. W takim przypadku, aby utworzyć kopię zapasową trzeciej partycji, w polu Wolumin można wpisać `/dev/hda3` lub `/home/usr/docs`.

Ogólnie rzecz biorąc, konfigurując scentralizowany plan tworzenia kopii zapasowych woluminów na komputerach z systemem Linux, w regułach wyboru woluminów należy wprowadzić ścieżki odpowiadające partycjom (takie jak `/dev/hda2` lub `/home/usr/docs` z poprzedniego przykładu), a nie katalogom.

Standardowe nazwy partycji systemu Linux

Nazwy, takie jak `/dev/hda1`, odzwierciedlają standardowy sposób nadawania nazw partycjom dysków twardych IDE w systemie Linux. Przedrostek **hd** oznacza typ dysku (IDE), **a** oznacza pierwszy dysk twardy IDE w systemie, a **1** — pierwszą partycję na tym dysku.

Ogólnie standardowa nazwa partycji systemu Linux ma trzy składowe:

- **Typ dysku:** `hd` (dyski IDE), `sd` (dyski SCSI), `md` (programowe dyski RAID, na przykład woluminy dynamiczne)
- **Numer dysku:** `a` dla pierwszego dysku, `b` dla drugiego dysku itd.
- **Numer partycji na dysku:** `1` dla pierwszej partycji, `2` dla drugiej partycji itd.

Aby zagwarantować tworzenie kopii zapasowych wybranych dysków niezależnie od ich typu, w oknie dialogowym **Dane uwzględniane w kopii zapasowej** należy dodać trzy wpisy, po jednym dla każdego z możliwych typów. Aby na przykład utworzyć kopię zapasową pierwszego dysku twardego na każdym komputerze z systemem Linux podlegającym scentralizowanemu planowi tworzenia kopii zapasowych, warto dodać następujące reguły:

```
/dev/hda1
```

```
/dev/sda1
```

```
/dev/mda1
```

Nazwy woluminów logicznych

Aby utworzyć kopie zapasowe woluminów logicznych, nazywanych również woluminami LVM, określ ich pełne nazwy w regułach wyboru. Pełna nazwa woluminu logicznego obejmuje grupę woluminów, do której on należy.

Aby na przykład utworzyć kopie zapasowe dwóch woluminów logicznych: **lv_root** i **lv_bin**, które oba należą do grupy woluminów **vg_mymachine**, określ następujące reguły wyboru:

```
/dev/vg_mymachine/lv_root  
/dev/vg_mymachine/lv_bin
```

W celu wyświetlenia listy woluminów logicznych na komputerze użyj narzędzia **lvdisplay**. W naszym przykładzie dane wyjściowe będą podobne do następujących:

```

--- Logical volume ---
LV Name      /dev/vg_mymachine/lv_root
VG Name      vg_mymachine
...

--- Logical volume ---
LV Name      /dev/vg_mymachine/lv_bin
VG Name      vg_mymachine
...

```

Wskazówka: Aby móc automatycznie tworzyć informacje o strukturze woluminów podczas odzyskiwania, upewnij się, że dla każdego komputera do tworzenia kopii zapasowej został wybrany wolumin zawierający katalog **/etc/Acronis**. Aby uzyskać więcej informacji, zobacz „Zapisywanie informacji o strukturze woluminu”.

11.2.4 Wybór lokalizacji kopii zapasowej

Określ miejsce docelowe archiwów i zdefiniuj nazwy nowych archiwów kopii zapasowych.

1. Wybór miejsca docelowego archiwów

Wybierz miejsce przechowywania archiwów komputerów:

- **Przechowuj archiwa wszystkich komputerów w jednej lokalizacji**

- Aby utworzyć kopię zapasową danych w magazynie Acronis Online Backup Storage, kliknij **Zaloguj** i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę **Magazyn kopii zapasowych online** i wybierz konto.

Przed utworzeniem kopii zapasowej w magazynie online należy zakupić subskrypcję usługi tworzenia kopii zapasowych online oraz aktywować tę subskrypcję na komputerach, których kopię zapasową chcesz utworzyć. Usługa tworzenia kopii zapasowych online jest niedostępna w systemie Linux.

Usługa Acronis Backup & Recovery Online nie jest dostępna we wszystkich regionach. Aby uzyskać więcej informacji, kliknij tutaj: <http://www.acronis.pl/my/backup-recovery-online/ro>

- Aby przechowywać archiwa w skarbcu centralnym, rozwiń grupę **Skarbce** i kliknij skarbiec.
- Aby przechowywać archiwa w udziale sieciowym, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.
- Aby przechowywać archiwa na serwerze **FTP** lub **SFTP**, rozwiń odpowiednią grupę i kliknij odpowiedni serwer, a następnie wybierz folder, w którym będą przechowywane archiwa.

Zgodnie z oryginalną specyfikacją protokołu FTP poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako zwykły tekst. Oznacza to, że nazwę użytkownika i hasło można przechwycić przy użyciu programu do przechwytywania pakietów.

- **Przechowuj archiwum każdego komputera w określonym folderze na komputerze z agentem**

W polu **Ścieżka** wprowadź pełną ścieżkę do folderu. Folder ten należy wcześniej utworzyć na każdym komputerze, dla którego utworzono scentralizowany plan tworzenia kopii zapasowych.

- **Przechowuj archiwum każdego komputera w jego strefie Acronis Secure Zone**

Strefę Acronis Secure Zone należy wcześniej utworzyć na każdym komputerze, dla którego utworzono scentralizowany plan tworzenia kopii zapasowych. Aby uzyskać informacje dotyczące sposobu tworzenia strefy Acronis Secure Zone, zobacz Tworzenie strefy Acronis Secure Zone (s. 188).

2. Nadawanie nazw archiwom

Kopia zapasowa danych z każdego komputera zostanie utworzona w oddzielnym archiwum.

Program wygeneruje typową nazwę nowych archiwów i wyświetli ją w polu **Nazwa**. Nazwa wygląda następująco: *[Nazwa komputera]_Archiwum(N)*, gdzie *[Nazwa komputera]* oznacza nazwę komputera fizycznego lub maszyny wirtualnej, a *N* to numer kolejnego archiwum. Jeśli automatycznie wygenerowana nazwa jest nieodpowiednia, określ inną.

Jeśli dane do uwzględnienia w kopii zapasowej wybierasz z wielu komputerów, możesz użyć następujących zmiennych:

- *[Nazwa komputera]* — podstawienie za nazwę komputera. Użycie tej zmiennej jest obowiązkowe.
- *[Nazwa planu]* — podstawienie za nazwę scentralizowanego planu tworzenia kopii zapasowych. Użyj tej zmiennej w celu dodatkowego rozróżnienia archiwów za pomocą nazw planów tworzenia kopii zapasowych.
- *[Nazwa hosta wirtualnego]* — podstawienie za nazwę hosta maszyny wirtualnej. Użyj tej zmiennej w przypadkach, gdy dwie lub więcej maszyn wirtualnych działających na różnych hostach ma te same nazwy.

Przykład: Tworzysz scentralizowany plan tworzenia kopii zapasowych o przykładowej nazwie *KOPIASYSTEMU*, który zostanie wdrożony na trzech komputerach (na przykład *DZIALFIN1*, *DZIALFIN2*, *DZIALFIN3*). W polu **Nazwa** określasz ciąg *[Nazwa komputera]_[Nazwa planu]_Archiwum(N)*. W ten sposób w lokalizacji zostaną utworzone następujące trzy archiwa:

- *DZIALFIN1_KOPIASYSTEMU_Archiwum(1)*
- *DZIALFIN2_KOPIASYSTEMU_Archiwum(1)*
- *DZIALFIN3_KOPIASYSTEMU_Archiwum(1)*

11.2.5 Poświadczenia scentralizowanego planu tworzenia kopii zapasowych

Wprowadź poświadczenia umożliwiające uruchomienie zadań scentralizowanych na komputerach.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń usługi Acronis**

Zadanie będzie wykonywane z konta usługi Acronis, niezależnie od tego, czy zostanie uruchomione ręcznie czy według harmonogramu.

- **Użyj następujących poświadczeń**

Zadanie będzie wykonywane z poświadczeniami określonymi przez użytkownika, niezależnie od tego, czy zostanie uruchomione ręcznie czy według harmonogramu.

Określ:

- **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (*DOMENA\Nazwa_użytkownika* lub *Nazwa_użytkownika@domena*).
- **Hasło.** Hasło dla konta.

2. Kliknij **OK**.

Aby dowiedzieć się więcej na temat poświadczeń usługi Acronis, zobacz sekcję Prawa dotyczące usług Acronis (s. 310).

Aby dowiedzieć się więcej na temat operacji dostępnych w zależności od uprawnień użytkownika, zobacz sekcję Uprawnienia użytkownika na komputerze zarządzanym (s. 33).

11.2.6 Co zrobić, jeśli na komputerze nie ma danych spełniających reguły wyboru

Scentralizowany plan tworzenia kopii zapasowych można wdrożyć na komputerze, na którym nie ma danych spełniających reguły wyboru. Podczas wdrażania planu nie są rejestrowane błędy ani ostrzeżenia, ponieważ przyjmuje się, że odpowiednie dane mogą się pojawić w przyszłości. Plan tworzenia kopii zapasowych powstaje w normalny sposób i jego stan zmienia się na **Wdrożone**.

Jeśli w chwili rozpoczęcia zadania program nie znajdzie danych do utworzenia kopii zapasowej, plan zakończy się niepowodzeniem, a status zasad zmieni się na **Błąd**. Jeśli program znajdzie co najmniej jeden z elementów danych, zadanie tworzenia kopii zapasowych zakończy się powodzeniem z ostrzeżeniem. Nastąpi również odpowiednia zmiana statusu planu.

Zadania tworzenia kopii zapasowych będą uruchamiane zgodnie z harmonogramem określonym przez plan i będą dawać podobny wynik, dopóki wszystkie elementy danych nie pojawią się na komputerze lub plan nie zostanie zmodyfikowany w celu wykluczenia nieistniejących elementów.

Przykłady

Przyjmijmy, że reguła wyboru określa, że plan ma powodować tworzenie kopii zapasowej woluminów D: i F:. Plan jest wdrożony na komputerach z systemami Linux oraz Windows. Po rozpoczęciu tworzenia pierwszej kopii zapasowej plan otrzymuje status **Błąd** na komputerach z systemem Linux oraz na tych komputerach z systemem Windows, które nie zawierają takich woluminów. Plan ma status **Ostrzeżenie** na komputerach z systemem Windows, na których znajduje się wolumin D: lub F:, chyba że wystąpi zdarzenie powodujące błąd.

Plan, który ma powodować tworzenie kopii zapasowej woluminów [SYSTEM] i /dev/sda1, będzie miał status **Ostrzeżenie** na komputerach z systemem Windows (ponieważ wolumin /dev/sda nie zostanie znaleziony) oraz na komputerach z systemem Linux, na których istnieje wolumin /dev/sda1. Dzieje się tak dlatego, że woluminu [SYSTEM] nie można znaleźć. Plan będzie miał status **Błąd** na komputerach z systemem Linux, na których nie ma urządzenia SCSI.

11.3 Administrowanie serwerem Acronis Backup & Recovery 11 Management Server

W tej sekcji opisano widoki dostępne za pośrednictwem drzewa nawigacji konsoli podłączonej do serwera zarządzania oraz wyjaśniono sposób pracy z każdym widokiem.

11.3.1 Pulpit nawigacyjny

Widok **Pulpit nawigacyjny** służy do szybkiej oceny, czy dane na zarejestrowanych komputerach są skutecznie chronione. Pulpit nawigacyjny przedstawia podsumowanie działań agentów Acronis Backup & Recovery 11, pozwala na sprawdzenie ilości wolnego miejsca dostępnego w skarbcach zarządzanych oraz umożliwia błyskawiczne identyfikowanie i rozwiązywanie ewentualnych problemów.

Ostatnie alerty

Sekcja **Ostatnie alerty** zwraca uwagę na problemy występujące na serwerze zarządzania, na zarejestrowanych komputerach i w skarbcach centralnych. Przedstawia ona sposoby ich analizy i naprawienia. Domyślnie w tej sekcji prezentowanych jest pięć ostatnich alertów. Kliknij łącze **Pokaż wszystko**, aby przejść do widoku **Alerty** i zapoznać się ze wszystkimi alertami. Jeśli nie ma żadnych alertów ani ostrzeżeń, wyświetlany jest komunikat „Brak alertów”.

Historia działań

Skumulowany wykres kolumnowy w sekcji **Historia działań** umożliwia zapoznanie się z dzienną historią działań agentów Acronis Backup & Recovery 11. Dane historyczne są oparte na wpisach dziennika gromadzonych z zarejestrowanych komputerów i serwera zarządzania. Wykres prezentuje liczbę wpisów dziennika każdego typu (**Wykonane pomyślnie**, **Z ostrzeżeniami**, **Zakończone niepowodzeniem**) dla określonego dnia.

Z prawej strony wykresu są wyświetlane informacje statystyczne dotyczące wybranej daty. Wszystkie pola statystyczne mają charakter interaktywny, tj. po kliknięciu dowolnego z nich otworzy się widok **Dziennik** z wpisami dziennika odfiltrowanymi na podstawie zawartości tego pola.

U góry wykresu można wybrać działania, które będą wyświetlane w zależności od obecności i wagi błędów. Kliknij łącze **Pokaż wszystko**, aby wyświetlić w widoku **Dziennik** wszystkie działania. Są one posortowane według daty rozpoczęcia. Prawym przyciskiem myszy kliknij określony dzień na wykresie kolumnowym, aby wyświetlić menu kontekstowe i przejść do widoku **Dziennik** odpowiadającego wybranej dacie.

Przycisk  **Dzisiaj** powoduje wybranie bieżącej daty.

Komputery, plany tworzenia kopii zapasowych i zadania odzyskiwania

Sekcje **Komputery**, **Plany tworzenia kopii zapasowych** i **Zadania odzyskiwania** przedstawiają podsumowanie informacji statystycznych dotyczących zarejestrowanych komputerów, planów tworzenia kopii zapasowych i zadań odzyskiwania. Klikaj elementy w tych sekcjach, aby uzyskać odpowiednie informacje. Powoduje to wyświetlenie właściwego widoku zawierającego odpowiednio wstępnie odfiltrowane komputery, plany tworzenia kopii zapasowych lub zadania odzyskiwania. Na przykład kliknięcie elementu **Wymagające działania** w obszarze **Zadania odzyskiwania** spowoduje otwarcie widoku **Plany i zadania tworzenia kopii zapasowych** zawierającego zadania odzyskiwania odfiltrowane według stanu **Wymagające działania**.

Informacje prezentowane w sekcjach **Komputery**, **Plany tworzenia kopii zapasowych** i **Zadania odzyskiwania** są odświeżane przy każdej synchronizacji serwera zarządzania z komputerami. Informacje w innych sekcjach są odświeżane co 10 minut oraz po każdym otwarciu Pulpitu nawigacyjnego.

Skarbcze

Sekcja **Skarbcze** prezentuje informacje dotyczące poziomu wykorzystania miejsca w skarbcach. W niektórych przypadkach informacje na temat ilości wolnego miejsca w skarbcu mogą być niedostępne, na przykład, gdy skarbiec znajduje się w bibliotece taśm. Jeśli niedostępny jest sam skarbiec (znajduje się w stanie offline), zostanie wyświetlony komunikat „Skarbiec jest niedostępny”.

W przypadku braku skarbców wyświetlany jest komunikat „Nie utworzono skarbców centralnych”. Aby utworzyć nowy skarbiec, wybierz łącze **Utwórz teraz** i przejdź do strony **Utwórz skarbiec**.

11.3.2 Komputery z agentami

Program Acronis Backup & Recovery 11 umożliwia ochronę danych i wykonywanie operacji zarządzania na wielu komputerach.

Dodaj komputer (s. 330) do serwera zarządzania za pomocą nazwy lub adresu IP komputera albo zaimportuj komputery z usługi Active Directory lub z plików tekstowych. Po zarejestrowaniu komputera na serwerze zarządzania może on zostać objęty scentralizowanym planem tworzenia kopii zapasowych (s. 315) oraz czynnościami grupowania i monitorowania związanymi z ochroną danych.

Aby ocenić, czy dane na komputerze zarządzanym są skutecznie chronione, sprawdź jego status. Status komputera jest najpoważniejszym statusem wszystkich planów tworzenia kopii zapasowych (s. 285) (lokalnych i scentralizowanych) istniejących na komputerze. Może on przyjmować wartość „OK”, „Ostrzeżenie” lub „Błąd”.


Typowy przepływ roboczy

- Utwórz grupę niestandardową i dodaj do niej komputery. Aby uzyskać więcej informacji, zobacz „Grupy komputerów” (s. 326).
- Aby wykonywać czynności dotyczące komputera (lub grupy), zaznacz go. Zobacz „Czynności dotyczące komputerów” (s. 327) i „Czynności dotyczące grup” (s. 335).
- Aby wyświetlić szczegółowe informacje na temat wybranego komputera lub grupy i wykonać dodatkowe operacje (takie jak uruchamianie i zatrzymywanie zadań czy importowanie i eksportowanie planów tworzenia kopii zapasowych), skorzystaj z panelu informacyjnego w dolnej części okna. Panel jest domyślnie zwinięty. Aby go rozwinąć, kliknij symbol strzałki (▲).
- Aby ułatwić przeglądanie i sprawdzanie wymaganych komputerów, skorzystaj z funkcji filtrowania i sortowania. Aby uzyskać więcej informacji, zobacz „Sortowanie, filtrowanie i konfigurowanie elementów tabeli” (s. 26).

Grupy komputerów

Grupy komputerów służą do wygodnej ochrony dużej liczby komputerów zarejestrowanych na serwerze zarządzania. Podczas tworzenia scentralizowanego planu tworzenia kopii zapasowych wystarczy wybrać grupę, a plan zostanie wdrożony na wszystkich komputerach do niej należących. Po pojawieniu się w grupie nowego komputera zostanie na nim wdrożony scentralizowany plan tworzenia kopii zapasowych. W przypadku usunięcia komputera z grupy zostanie z niego usunięty scentralizowany plan tworzenia kopii zapasowych. Pojedynczy komputer może być jednocześnie członkiem wielu grup.

Grupa wbudowana

Natychmiast po zarejestrowaniu na serwerze zarządzania komputer pojawi się w grupie wbudowanej  **Wszystkie komputery z agentami**. Grupa ta jest stale obecna na serwerze zarządzania i nie można jej edytować ani usunąć. Grupa wbudowana nie może zawierać żadnych grup zagnieżdżonych.

Aby jednocześnie objąć ochroną wszystkie zarejestrowane komputery, utwórz scentralizowany plan tworzenia kopii zapasowych i wybierz grupę **Wszystkie komputery z agentami**. Ochrona wszystkich komputerów z wykorzystaniem pojedynczego planu tworzenia kopii zapasowych może być niewystarczająca ze względu na różne role poszczególnych komputerów. Chronione dane każdego działu mają swoją specyfikę. Kopie zapasowe niektórych danych trzeba tworzyć bardzo często, a innych dwa razy do roku. Dobrym rozwiązaniem może być utworzenie różnych planów tworzenia kopii zapasowych dla różnych zestawów komputerów. W takim przypadku warto rozważyć utworzenie grup niestandardowych.

Grupy niestandardowe

Grupy niestandardowe tworzy administrator serwera zarządzania. Pozwala mu to organizować ochronę danych według działów firmy, jednostek administracyjnych usługi Active Directory, różnych grup użytkowników, miejsc itd.

Grupa niestandardowa może zawierać jedną lub więcej grup zagnieżdżonych. Każdą grupę niestandardową można edytować lub usunąć. Administrator może tworzyć następujące rodzaje grup niestandardowych:

■ Grupy statyczne

Grupy statyczne obejmują komputery dodane ręcznie przez administratora. Ich zawartość może zmienić się tylko wtedy, gdy administrator ręcznie doda lub usunie komputer.

Przykład: Tworzysz grupę niestandardową działu księgowości i ręcznie dodajesz do niej komputery księgowych. Komputery księgowych zostaną objęte ochroną po utworzeniu dla tej grupy scentralizowanego planu tworzenia kopii zapasowych. Po zatrudnieniu nowej osoby w tym dziale trzeba będzie ręcznie dodać nowy komputer do grupy.

■ Grupy dynamiczne

Grupy dynamiczne obejmują komputery dodawane automatycznie na podstawie kryteriów określonych przez administratora. Zawartość grupy dynamicznej zmienia się automatycznie. Komputery należą do grupy tak długo, jak długo spełniają określone kryteria.

Przykład: Dział księgowości stanowi odrębną jednostkę organizacyjną usługi Active Directory. Wystarczy określić jednostkę organizacyjną księgowości jako kryterium członkostwa w grupie i utworzyć scentralizowany plan tworzenia kopii zapasowych dla grupy. W przypadku zatrudnienia nowego księgowego nowy komputer zostanie dodany do grupy z chwilą dodania go do jednostki organizacyjnej, a następnie automatycznie objęty ochroną.


Wskazówka. Aby optymalnie wykorzystać kryterium jednostki organizacyjnej usługi Active Directory, warto odtworzyć hierarchię usługi Active Directory na serwerze zarządzania.



Więcej informacji na temat operacji dotyczących grup i komputerów zawierają następujące sekcje:



- Czynności dotyczące grup (s. 335)
- Czynności dotyczące komputerów (s. 327)


Czynności dotyczące komputerów

Rejestrowanie komputerów na serwerze zarządzania

Po dodaniu lub zaimportowaniu komputera do grupy  **Wszystkie komputery z agentami** zostanie on zarejestrowany na serwerze zarządzania. Na zarejestrowanych komputerach można wdrożyć scentralizowane plany tworzenia kopii zapasowych i wykonać inne operacje zarządzania scentralizowanego. Rejestracja polega na ustanowieniu relacji zaufania między agentem znajdującym się na komputerze i serwerem.

Po wybraniu widoku  **Komputery z agentami** lub grupy  **Wszystkie komputery z agentami** w drzewie Nawigacja dostępne staną się czynności dodawania i importowania.


Zadanie	Czynności
Dodawanie nowego komputera do serwera zarządzania	Kliknij  Dodaj komputer do AMS. W oknie Dodaj komputer (s. 330) wybierz komputer, który trzeba dodać do serwera zarządzania.
Dodawanie wielu	Kliknij  Dodaj wiele komputerów.

Zadanie	Czynności
komputerów	<p>Określ komputery, które chcesz dodać do serwera zarządzania. W ten sposób można dodawać komputery z systemem Windows bez zainstalowanego agenta. Agent dla systemu Windows zostanie zainstalowany automatycznie za pomocą funkcji instalacji zdalnej.</p> <p>Aby uzyskać szczegółowe informacje, zobacz „Określanie listy komputerów” w dokumentacji instalacji.</p>
Synchronizowanie komputerów z listą w pliku tekstowym	<p>Kliknij  Synchronizuj z plikiem.</p> <p>Określ plik tekstowy zawierający listę komputerów. Po zakończeniu synchronizacji na serwerze zarządzania pozostaną zarejestrowane tylko te komputery, które są wymienione w pliku. Aby uzyskać szczegółowe informacje, zobacz „Synchronizowanie komputerów z plikiem tekstowym” (s. 330).</p>






Konsola zarządzania kontaktuje się z agentem i rozpoczyna procedurę rejestracji. Ponieważ rejestracja wymaga uczestnictwa agenta, nie jest możliwa, gdy komputer jest w trybie offline.


Dodatkowy agent, który jest zainstalowany na zarejestrowanym komputerze, automatycznie staje się zarejestrowany na tym samym serwerze zarządzania. Istnieje możliwość jednoczesnego rejestrowania i wyrejestrowywania wielu agentów.

Usuwanie wybranego komputera z serwera zarządzania




Zadanie	Czynności
Usunięcie komputera z serwera zarządzania	<p>Kliknij  Usuń komputer z AMS.</p> <p>W rezultacie plany tworzenia kopii zapasowych zostaną usunięte, a skróty do skarbów centralnych zostaną usunięte z komputera. Jeśli komputer nie jest aktualnie dostępny, działania te zostaną wykonane na komputerze zaraz po tym, gdy stanie się on dostępny dla serwera.</p>

Działania grupowania





Zadanie	Czynności
Utworzenie niestandardowej grupy statycznej lub dynamicznej	<p>Kliknij  Utwórz grupę.</p> <p>W oknie Utwórz grupę (s. 336) określ wymagane parametry grupy. Nowa grupa zostanie utworzona w grupie, do której należy wybrany komputer (nie dotyczy to wbudowanej grupy  Wszystkie komputery z agentami).</p>
Dodawanie komputera do innej grupy statycznej.	<p>Kliknij  Dodaj do innej grupy.</p> <p>W oknie Dodaj do grupy (s. 332) określ grupę, do której chcesz skopiować wybrany komputer. Na komputerze wdrożone zostaną scentralizowane plany tworzenia kopii zapasowych stosowane do grup, do których należy komputer.</p>
Dla komputerów grupach niestandardowych	
Dodawanie maszyny do grupy statycznej	<p>Kliknij  Dodaj komputery do grupy.</p> <p>W oknie Dodaj komputery do grupy (s. 332) wybierz komputery, które chcesz dodać. Scentralizowane plany tworzenia kopii zapasowych stosowane do grup zostaną wdrożone na wybranych komputerach.</p>
Przenoszenie komputera do innej grupy statycznej.	<p>Kliknij  Przenieś do innej grupy.</p> <p>W oknie Przenieś do grupy (s. 332) wybierz grupę, do której komputer ma być</p>


Zadanie	Czynności
	przeniesiony. Zostaną usunięte wszystkie scentralizowane plany tworzenia kopii zapasowych stosowane do grupy, do której wcześniej należał komputer. Na komputerze zostaną wdrożone scentralizowane plany tworzenia kopii zapasowych stosowane do grupy, do której teraz należy komputer.
Usuwanie komputera z bieżącej grupy statycznej	Kliknij  Usuń z grupy . Scentralizowane plany tworzenia kopii zapasowych stosowane do grupy zostaną automatycznie usunięte z komputera.

Zarządzanie bezpośrednie

Zadanie	Czynności
Tworzenie planu kopii zapasowych na komputerze	Kliknij  Utwórz kopię zapasową . Operację tę opisano szczegółowo w sekcji Tworzenie planu tworzenia kopii zapasowych (s. 48).
Odzyskiwanie danych	Kliknij  Odzyskaj . Operację tę opisano szczegółowo w sekcji Odzyskiwanie danych (s. 130).
Bezpośrednie połączenie z komputerem	Kliknij  Połącz bezpośrednio . Pozwala nawiązać bezpośrednie połączenie z komputerem zarządzanym. Umożliwia administrowanie komputerem zarządzanym i wykonanie wszystkich operacji zarządzania bezpośredniego (s. 389).

Inne działania



Zadanie	Czynności
Wyświetlenie szczegółowych informacji o komputerze	Kliknij  Szczegóły . W oknie Szczegóły komputera (s. 333) zapoznaj się z informacjami o danym komputerze.
Wyświetlenie pozycji dziennika dla komputera	Kliknij  Dziennik . W widoku Dziennik (s. 352) zostanie przedstawiona lista wpisów dziennika komputera.
Aktualizacja licencji agenta komputera	Kliknij  Zmień licencję . Używaj funkcji Zmień licencję w następujących przypadkach <ul style="list-style-type: none"> ▪ przejście z próbnej wersji programu do pełnej, ▪ aby włączyć funkcję Acronis Deduplication, ▪ aby włączyć funkcję Acronis Universal Restore.
Aktualizacja wszystkich informacji związanych z komputerem	Kliknij  Synchronizuj . Serwer zarządzania uzyska z komputera najbardziej aktualne informacje o nim i zsynchronizuje je z bazą danych. Dodatkowo, poza synchronizacją, jednocześnie zostanie wykonane odświeżenie listy komputerów.

Zadanie	Czynności
Odświeżenie listy komputerów	<p>Kliknij  Odśwież.</p> <p>Konsola zarządzania wykona aktualizację listy komputerów o najnowsze informacje z serwera zarządzania. Mimo że lista zadań jest odświeżana automatycznie na podstawie zdarzeń, ze względu na pewne opóźnienie dane z serwera zarządzania mogą nie pojawić się natychmiast. Po ręcznym odświeżeniu wyświetlane są najbardziej aktualne dane.</p>

Dodawanie komputera do serwera zarządzania

Aby umożliwić wdrażanie scentralizowanych planów tworzenia kopii zapasowych z serwera zarządzania Acronis Backup & Recovery 11 Management Server na zarządzanym komputerze i wykonywanie innych operacji zarządzania scentralizowanego, należy zarejestrować komputer na serwerze zarządzania.

Aby dodać komputer

1. W drzewie Nawigacja wybierz  **Komputery z agentami**.
2. Kliknij  **Dodaj komputer do AMS** na pasku narzędzi.
3. W polu **Adres IP/nazwa** wprowadź nazwę komputera lub jego adres IP albo kliknij **Przeglądaj** i wyszukaj komputer w sieci.

Uwaga dla użytkowników wersji Virtual Edition: W przypadku dodawania hosta VMware ESX(i) wprowadź adres IP urządzenia wirtualnego lub komputera z systemem Windows, na którym jest uruchomiony komponent Acronis Backup & Recovery 11 Agent for ESX(i).

4. Określ nazwę i hasło użytkownika należącego do grupy **Administratorzy** na komputerze.

Uwaga dla użytkowników wersji Virtual Edition: W przypadku dodawania hosta VMware ESX(i) określ nazwę i hasło użytkownika serwera vCenter Server lub hosta ESX(i).

 - **Nazwa użytkownika.** Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika).
 - **Hasło.** Hasło konta.


Zaznacz pole wyboru **Zapisz hasło**, aby zapamiętać hasło dla kolejnych połączeń.
5. Kliknij **Dalej**, a następnie kliknij **Kontynuuj**.

Inicjowanie rejestracji po stronie komputera

Procedurę rejestracji można zainicjować po stronie komputera.

1. Podłącz konsolę do komputera, na którym jest zainstalowany agent Acronis Backup & Recovery 11. W przypadku wyświetlenia pytania o poświadczenia określ poświadczenia członka grupy **Administratorzy** na komputerze.
2. Z menu wybierz **Opcje > Opcje komputera > Zarządzanie komputerem**.
3. Wybierz **Zarządzanie scentralizowane** i określ serwer zarządzania, na którym chcesz zarejestrować komputer. Aby uzyskać szczegółowe informacje, zobacz „Zarządzanie komputerem (s. 302)”.

Synchronizacja komputerów z plikiem tekstowym

W czasie synchronizacji serwer zarządzania dopasowuje grupę  **Wszystkie komputery z agentami** do listy komputerów umieszczonej w pliku .txt lub .csv. Serwer zarządzania:

- Dodaje komputery, które znajdują się na liście, ale nie są zarejestrowane.

- Usuwa zarejestrowane komputery, który nie znajdują się na liście.
- Usuwa i próbuje ponownie dodać zarejestrowane komputery, które znajdują się na liście, ale ich bieżąca dostępność (s. 333) jest określona jako **Wycofany**.

Oznacza to, że w grupie **Wszystkie komputery z agentami** będą się znajdować tylko te komputery, które są umieszczone w pliku.

Wymagania dotyczące pliku tekstowego

Plik powinien zawierać po jednej nazwie lub jednym adresie IP komputera w każdym wierszu.

Przykład:

```
Machine_name_1
Machine_name_2
192.168.1.14
192.168.1.15
```




Określenie pustego pliku powoduje usunięcie z serwera zarządzania wszystkich komputerów z agentami.

Zarejestrowany komputer musi być określony za pomocą jego adresu rejestracji. Oznacza to, że należy podać dokładnie tę samą nazwę hosta, pełną kwalifikowaną nazwę domeny (FQDN) lub adres IP, co podczas początkowego dodawania komputera do serwera zarządzania. W przeciwnym razie komputer zostanie usunięty i dodany jako nowy. Oznacza to, że z komputera zostaną usunięte wszystkie scentralizowane plany tworzenia kopii zapasowych, odziedziczone i wdrożone bezpośrednio, oraz że utraci on członkostwo w grupach statycznych.

Adres rejestracji każdego komputera znajduje się w kolumnie **Adres rejestracji** w dowolnym widoku serwera zarządzania obejmującym dany komputer (kolumna ta jest domyślnie ukryta).

Aby uniknąć rozbieżności, można na początku wykonać import komputerów z pliku tekstowego. Plik ten można później zmodyfikować przez dodanie lub usuwanie komputerów. Nie należy jednak zmieniać nazw lub adresów tych komputerów, które mają pozostać zarejestrowane.

Aby zsynchronizować komputery z plikiem tekstowym

1. W drzewie **Nawigacja** wybierz  **Komputery z agentami** lub  **Wszystkie komputery z agentami**.
2. Na pasku narzędzi kliknij  **Synchronizuj z plikiem**.
3. W polu **Ścieżka** wprowadź ścieżkę do pliku .txt lub .csv albo kliknij **Przeglądaj** i w oknie **Przeglądaj** wybierz plik.
4. W opcji **Ustawienia logowania** określ nazwę i hasło użytkownika należącego do grupy Administratorzy na wszystkich komputerach umieszczonych w pliku.
5. Aby rozpocząć importowanie, kliknij **OK**.

Narzędzie wiersza polecenia do synchronizacji

Serwer zarządzania Acronis Backup & Recovery 11 Management Server udostępnia narzędzie wiersza polecenia, które umożliwia utworzenie pliku wsadowego i zaplanowanie zadania synchronizacji przy użyciu harmonogramu systemu Windows.

Aby zsynchronizować maszyny za pomocą pliku tekstowego przy użyciu wiersza polecenia

1. Zaloguj się jako członek grupy zabezpieczeń **Acronis Centralized Admins**.

2. W wierszu polecenia zmień katalog na folder, w którym został zainstalowany serwer zarządzania Acronis Backup & Recovery 11 Management Server. Domyślnie jest to folder **C:\Program Files\Acronis\AMS**.

3. Uruchom następujące polecenie:

```
syncmachines [path_to_the_file] {username password}
```

gdzie:

- [ścieżka_do_pliku] to ścieżka do pliku txt lub csv zawierającego listę maszyn. Narzędzie nie obsługuje spacji w nazwie ścieżki.
- {nazwa_użytkownika hasło} należy do użytkownika, który jest członkiem grupy administratorów na wszystkich maszynach znajdujących się na liście w pliku. Jeśli nie określono inaczej, na wszystkich maszynach będzie używany mechanizm rejestracji jednokrotnej.

Dodawanie komputera do innej grupy

Aby dodać wybrany komputer do innej grupy

1. Wybierz grupę, do której ma zostać dodany komputer.
2. Kliknij **OK**.

Dodawany komputer stanie się członkiem wielu grup. W rezultacie scentralizowane plany tworzenia kopii zapasowych dla pierwszej grupy pozostaną na komputerze, natomiast scentralizowane plany tworzenia kopii zapasowych utworzone dla grupy drugiej, trzeciej i kolejnych zostaną na nim także wdrożone.

Przenoszenie komputera do innej grupy

Aby przenieść wybrany komputer do innej grupy

1. W drzewie grup wybierz grupę, do której zostanie przeniesiony komputer.
2. Kliknij **OK**.

Przenoszony komputer opuszcza jedną grupę i staje się członkiem innej. W wyniku tej operacji z komputera zostaną usunięte scentralizowane plany tworzenia kopii zapasowych utworzone dla pierwszej grupy, natomiast wdrożone na nim zostaną scentralizowane plany tworzenia kopii zapasowych stosowane w drugiej grupie.

Dodawanie komputerów do grupy

Aby dodać komputery do wybranej grupy

1. W drzewie grup wybierz grupę, której komputery musisz dodać.
2. W prawej części okna wybierz komputery.
3. Aby dodać więcej komputerów z innych grup, powtórz kroki 1 i 2 dla każdej grupy.
4. Kliknij **OK**, aby dodać komputery.

Po pojawieniu się komputerów w grupie zostaną na nich wdrożone scentralizowane plany tworzenia kopii zapasowych utworzone dla tej grupy (jeśli takie istnieją). Jeśli w danym momencie którykolwiek z wybranych komputerów jest niedostępny lub nieosiągalny, czynność ta zostanie zachowana na serwerze zarządzania jako czynność oczekująca i będzie wykonana zaraz po udostępnieniu komputera serwerowi.

Szczegóły komputera

Na czterech kartach znajdują się wszystkie informacje dotyczące wybranego komputera, które umożliwiają administratorowi serwera zarządzania wykonywanie operacji związanych z planami i zadaniami tworzenia kopii zapasowych na komputerze.

Komputer

Na tej karcie są wyświetlane następujące informacje dotyczące zarejestrowanego komputera:

- **Nazwa** — nazwa wybranego komputera (pobrana z pola **Nazwa komputera** w systemie Windows).
- **Adres rejestracji** — nazwa lub adres IP wybranego komputera. W trakcie rejestrowania komputera (s. 383) administrator serwera zarządzania może przypisać nazwę lub adres IP identyfikujący komputer na serwerze zarządzania.
- **Adres IP** — adres IP wybranego komputera.
- **System operacyjny** — system operacyjny uruchomiony w agencie komputera.
- **Status kondycji dysku** — stan kondycji dysków komputera. Jeśli na komputerze nie ma zainstalowanego narzędzia Acronis Drive Monitor, pole to ma wartość **Niedostępny**. Narzędzie Acronis Drive Monitor automatycznie sprawdza dyski w poszukiwaniu problemów i prognozuje termin awarii dysku twardego. Narzędzie to jest bezpłatne i można je pobrać ze strony <http://www.acronis.pl>.
- **Łączny postęp** — stan zadania. Wyświetla pasek postępu, jeśli zadanie znajduje się w stanie **Uruchomione**.
- **Status** — status komputera. Określony jako najpoważniejszy status (s. 285) wszystkich planów tworzenia kopii zapasowych (lokalnych i scentralizowanych) istniejących na komputerze.
- **Ostatnie połączenie** — czas, który upłynął od ostatniego połączenia serwera zarządzania z komputerem.
- **Ostatnia pomyślnie utworzona kopia zapasowa** — czas, który upłynął od ostatniego pomyślnego utworzenia kopii zapasowej.
- **Następna kopia zapasowa** — czas, który pozostał do utworzenia następnej kopii zapasowej.
- **Dostępność:**
 - **Online** — komputer jest dostępny dla serwera zarządzania. Oznacza to, że ostatnie połączenie serwera zarządzania z komputerem zostało nawiązane pomyślnie. Próby połączeń są wykonywane co dwie minuty.
 - **Offline** — komputer nie jest dostępny dla serwera zarządzania: został wyłączony lub odłączono od niego kabel sieciowy.
 - **Nieznany** — ten stan jest wyświetlany po dodaniu komputera lub uruchomieniu usługi serwera zarządzania, a przed pierwszym połączeniem serwera z komputerem.
 - **Wycofany** — komputer został zarejestrowany na innym serwerze zarządzania lub w ustawieniu **Opcje > Opcje komputera > Zarządzanie komputerem** (s. 302) został wybrany parametr **Zarządzanie autonomiczne**. Oznacza to, że nie jest możliwe sterowanie komputerem z bieżącego serwera zarządzania. Aby odzyskać możliwość sterowania komputerem, należy określić adres serwera zarządzania w ustawieniach **Zarządzanie komputerem**.
 - **Wygaś** — upłynął okres próbny agenta komputera. Aby określić pełny klucz licencyjny, użyj funkcji **Zmień licencję** lub uruchom program instalacyjny i postępuj zgodnie z jego instrukcjami.

- **Zainstalowane agenty** — pełne nazwy zainstalowanych na komputerze agentów programu Acronis.
- **Procesor** — typ procesora w zarządzanym komputerze.
- **Zegar procesora** — szybkość taktowania procesora.
- **Pamięć RAM** — rozmiar pamięci.
- **Opis** — opis komputera (pobrany z pola **Opis komputera** w systemie Windows).

Plany i zadania tworzenia kopii zapasowych

Pokazuje listę planów (lokalnych i centralnych) oraz zadań istniejących na wybranym komputerze.

Operacje

Aby uzyskać listę operacji dostępnych dla planów i zadań tworzenia kopii zapasowych komputera, zobacz „Czynności dotyczące planów i zadań tworzenia kopii zapasowych” (s. 282).




Filtrowanie i sortowanie

Filtrowanie i sortowanie planów i zadań tworzenia kopii zapasowych jest realizowane zgodnie z opisem w sekcji „Sortowanie, filtrowanie i konfigurowanie elementów tabeli” (s. 26).

Członek grupy

Karta pojawia się tylko po dodaniu wybranego komputera do jednej lub więcej grup niestandardowych i wyświetla listę grup, których członkiem jest komputer.

Operacje

Zadanie	Czynności
Wyświetl szczegóły grupy	Kliknij  Szczegóły . Nastąpi przeniesienie do okna Szczegóły grupy , gdzie można zapoznać się ze wszystkimi informacjami dotyczącymi grupy.
Usuwanie komputera z grupy	Kliknij  Usuń z tej grupy . Plany scentralizowane wdrożone w grupie nadrzędnej nie będą już miały wpływu na ten komputer.
Odświeżanie listy grup	Kliknij  Odśwież . W trakcie przeglądania informacji o komputerze może dojść do dodania, usunięcia lub modyfikacji wyświetlanych grup. Kliknij Odśwież , aby w informacjach dotyczących grup uwzględnić najnowsze zmiany. Spowoduje to otwarcie widoku Dziennik za wstępnie odfiltrowanymi wpisami dziennika dotyczącymi wybranej grupy.

Postęp


Na karcie **Postęp** znajduje się lista wszystkich czynności i zadań aktualnie uruchomionych na wybranym komputerze. Zawiera ona informacje na temat postępu realizacji zadań, czasu, który upłynął, oraz pozostałych parametrów.

Zarządzane maszyny wirtualne













Na tej karcie wyświetlana jest lista maszyn obsługiwanych na wybranym serwerze wirtualizacji lub zarządzanych przez określone urządzenie wirtualne.





Na podstawie listy obsługiwanych maszyn wirtualnych można utworzyć grupę dynamiczną. W tym celu kliknij **Utwórz grupę dynamiczną**. Utworzona grupa będzie dostępna w widoku Maszyny wirtualne.

Czynności dotyczące grup

Czynności stają się dostępne po wybraniu widoku  **Komputery z agentami** w drzewie **Nawigacja**. Aby wykonać czynność dotyczącą grupy, należy wybrać grupę w drzewie **Nawigacja** lub w widoku **Komputery z agentami**.

Poniżej przedstawiono wskazówki dotyczące wykonywania czynności dotyczących wybranych grup.

Zadanie	Czynności
Dodawanie komputera do serwera zarządzania	<p>Ta czynność jest dostępna tylko dla widoku  Komputery z agentami i dla grupy  Wszystkie komputery z agentami.</p> <p>Kliknij  Dodaj komputer do AMS.</p> <p>W oknie Dodaj komputer (s. 330) wybierz komputer, który trzeba dodać do serwera zarządzania.</p>
Synchronizowanie komputerów z listą w pliku tekstowym	<p>Ta czynność jest dostępna tylko dla widoku  Komputery z agentami i dla grupy  Wszystkie komputery z agentami.</p> <p>Kliknij  Synchronizuj z plikiem.</p> <p>Określ plik tekstowy zawierający listę komputerów. Po zakończeniu synchronizacji na serwerze zarządzania pozostaną zarejestrowane tylko te komputery, które są wymienione w pliku. Aby uzyskać więcej informacji, zobacz „Synchronizowanie komputerów z plikiem tekstowym (s. 330)”.</p>
Tworzenie niestandardowej grupy statycznej lub dynamicznej	<p>Kliknij  Utwórz grupę.</p> <p>W oknie Utwórz grupę (s. 336) określ wymagane parametry grupy.</p> <p>Grupy niestandardowe można tworzyć w folderze głównym ( Komputery z agentami) lub w innych grupach niestandardowych.</p>
Dodawanie komputerów do wybranej grupy statycznej	<p>Kliknij  Dodaj komputery do grupy.</p> <p>W oknie Dodaj komputery do grupy (s. 332) wybierz komputery, które chcesz dodać.</p> <p>Nie dotyczy grup dynamicznych.</p>
Tworzenie nowego planu tworzenia kopii zapasowych dla grupy	<p>Kliknij  Utwórz plan tworzenia kopii zapasowych, aby utworzyć plan tworzenia kopii zapasowych dla wybranej grupy.</p> <p>Operację tę opisano szczegółowo w sekcji Tworzenie planu tworzenia kopii zapasowych (s. 48).</p>
Wyświetlanie szczegółowych informacji o grupie	<p>Kliknij  Szczegóły.</p> <p>W oknie Szczegóły grupy (s. 338) zapoznaj się z informacjami o wybranej grupie.</p>
Zmiana nazwy grupy niestandardowej lub podrzędnej	<p>Kliknij  Zmień nazwę.</p> <p>W kolumnie Nazwa wpisz nową nazwę wybranej grupy.</p> <p>Nie można zmienić nazw grup wbudowanych.</p>

Zadanie	Czynności
Edycja grupy niestandardowej	Kliknij  Edytuj . W oknie Edytuj grupę (s. 338) zmień wymagane parametry grupy.
Przenoszenie grupy niestandardowej do innej grupy	Kliknij  Przenieś do . W oknie Przenieś do grupy (s. 338) określ grupę, która stanie się nową grupą nadrzędną wybranej grupy.
Usuwanie grupy niestandardowej	Kliknij  Usuń . Usunięcie grupy nadrzędnej spowoduje również usunięcie jej grup podrzędnych. Scentralizowane plany tworzenia kopii zapasowych utworzone dla grupy nadrzędnej i odziedziczone przez jej grupy podrzędne zostaną usunięte ze wszystkich członków usuwanych grup. Pozostaną tylko plany tworzenia kopii zapasowych utworzone bezpośrednio dla poszczególnych członków.
Odświeżanie listy grup	Kliknij  Odśwież . Konsola zarządzania zaktualizuje listę grup o najnowsze informacje z serwera zarządzania. Mimo że lista grup jest odświeżana automatycznie na podstawie zdarzeń, ze względu na pewne opóźnienie dane z serwera zarządzania mogą nie pojawić się natychmiast. Po ręcznym odświeżeniu wyświetlane są najbardziej aktualne dane.

Tworzenie niestandardowej grupy statycznej lub dynamicznej

Aby utworzyć grupę

- W polu **Nazwa** wprowadź nazwę tworzonej grupy.
- Wybierz typ grupy:
 - Statyczny** — aby utworzyć grupę, do której komputery będą dodawane ręcznie.
 - Dynamiczny** — aby utworzyć grupę, która będzie zawierać komputery dodawane automatycznie na podstawie określonych kryteriów.
Kliknij **Dodaj kryterium** i wybierz wzorzec kryterium.
 - System operacyjny**,
Członkami grupy dynamicznej będą wszystkie komputery działające pod kontrolą wybranego systemu operacyjnego.
 - Jednostka organizacyjna** (s. 337)
Członkami grupy dynamicznej będą wszystkie komputery należące do określonej jednostki organizacyjnej (OU).
 - Zakres adresów IP**
Członkami grupy dynamicznej będą wszystkie komputery z adresami IP z określonego zakresu.
 - Wymieniony w pliku .txt/.csv** (s. 337)
Do grupy dynamicznej będą należeć wszystkie komputery znajdujące się w określonym pliku .txt lub .csv.
- W polu **Opis grupy** wprowadź opis utworzonej grupy.
- Kliknij **OK**.

Dodawanie wielu kryteriów

Dodanie wielu kryteriów powoduje utworzenie warunku zgodnie z następującymi regułami:

- a) Wszystkie wpisy tego samego kryterium łączy się za pomocą dodawania logicznego (LUB).

Na przykład następujący zestaw kryteriów:

System operacyjny: Windows Server 2008

System operacyjny: Windows Server 2003

spowoduje dodanie do tej samej grupy wszystkich komputerów z systemem operacyjnym Windows 2000 LUB Windows 2003.

- b) Wpisy różnych kryteriów łączy się za pomocą mnożenia logicznego (I).

Weź na przykład pod uwagę następujący zestaw kryteriów:

System operacyjny: Windows Server 2008

System operacyjny: Windows Server 2003

Jednostka organizacyjna: SERVERS

Zakres adresów IP: 192.168.17.0 - 192.168.17.55

Kryteria ta spowodują dodanie do tej samej grupy wszystkich komputerów z systemem operacyjnym Windows 2000 lub Windows 2003, należących do jednostki organizacyjnej SERVERS oraz z adresami IP z zakresu 192.168.17.0 – 192.168.17.55.

Kryterium jednostki organizacyjnej

Kryterium jednostki organizacyjnej jest określone dla domeny, w której aktualnie znajduje się serwer zarządzania. Kryterium wygląda w następujący sposób: **OU=OU1**

Wybierz jednostkę organizacyjną z drzewa Active Directory, klikając **Przeglądaj**, lub wprowadź ją ręcznie. Jeśli w opcjach serwera zarządzania nie zostały określone poświadczenia dostępu do domeny, program poprosi o ich wprowadzenie. Poświadczenia zostaną zapisane w opcji Poświadczenia umożliwiające uzyskanie dostępu do domeny (s. 356).

Przypuśćmy, że domena *us.corp.przyklad.com* ma jednostkę organizacyjną OU1 (która jest na poziomie głównym), OU1 ma OU2, a OU2 ma OU3. Chcesz dodać komputery z jednostki OU3. Kryterium będzie wyglądać w następujący sposób: **OU=OU3, OU=OU2, OU=OU1**

Jeśli jednostka OU3 zawiera kontenery podrzędne i chcesz dodać komputery z tych kontenerów do grupy, zaznacz pole wyboru **Uwzględnij kontenery podrzędne**.

Kryterium Wymieniony w pliku txt/csv

Jeśli użyjesz tego kryterium, grupa dynamiczna obejmie komputery z listy podanej w określonym pliku .txt lub .csv.

W przypadku późniejszej modyfikacji tego pliku zawartość grupy ulegnie odpowiedniej zmianie. Plik jest sprawdzany co 15 minut.

Późniejsze usunięcie tego pliku lub jego niedostępność spowoduje, że zawartość grupy będzie odpowiadać liście ostatnio przechowywanej w pliku.

Wymagania dotyczące pliku tekstowego

Plik powinien zawierać po jednej nazwie lub jednym adresie IP komputera w każdym wierszu.

Przykład:

```
Nazwa_komputera_1
Nazwa_komputera_2
192.168.1.14
192.168.1.15
```

Zarejestrowany komputer musi być określony za pomocą swojego adresu rejestracji. Oznacza to, że należy podać dokładnie tę samą nazwę hosta, w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP, które określono podczas początkowego dodawania komputera do serwera zarządzania. W przeciwnym przypadku komputer nie zostanie dodany do grupy. Adres rejestracji każdego komputera znajduje się w kolumnie **Adres rejestracji** w dowolnym widoku serwera zarządzania obejmującym dany komputer (kolumna ta jest domyślnie ukryta).

Przenoszenie grupy do innej grupy

Aby przenieść wybraną grupę do innej grupy lub folderu głównego

1. W drzewie grup kliknij grupę, do której chcesz przenieść wybraną grupę. Program umożliwia przenoszenie grup niestandardowych dowolnego typu (statycznych lub dynamicznych) do innej grupy niestandardowej dowolnego typu lub do folderu głównego.

Folder główny drzewa komputerów zawiera *grupy pierwszego poziomu*. Grupy obejmujące inne grupy są określane mianem *grup nadrzędnych*. Grupy znajdujące się w grupach nadrzędnych są określane mianem *grup podrzędnych*. Wszystkie scentralizowane plany tworzenia kopii zapasowych utworzone dla grupy nadrzędnej zostaną także wdrożone na komputerach jej grup podrzędnych.

2. Kliknij **OK**.

Edytowanie grup niestandardowych

Edycja grupy niestandardowej odbywa się w ten sam sposób co jej tworzenie (s. 336).

Zmiana typu grupy spowoduje jej konwersję. Dowolną niestandardową grupę statyczną można przekonwertować na grupę dynamiczną lub odwrotnie.

- Podczas konwersji grupy statycznej na dynamiczną należy określić kryteria grupowania. Z grupy dynamicznej zostaną usunięci wszyscy członkowie istniejący w grupie statycznej, którzy nie spełniają określonych kryteriów.
- Podczas konwersji grupy dynamicznej na statyczną dostępne są dwie opcje: można pozostawić bieżącą zawartość grupy lub opróżnić grupę.

Szczegóły grupy

Na dwóch kartach znajdują się wszystkie informacje dotyczące wybranej grupy. Pozwalają one na wykonywanie operacji związanych ze scentralizowanymi planami tworzenia kopii zapasowych dla grupy.






Grupa

Na tej karcie są wyświetlane następujące informacje dotyczące grupy:

- **Nazwa** — nazwa wybranej grupy
- **Grupa nadrzędna** (tylko w przypadku podgrup) — nazwa grupy nadrzędnej
- **Komputery** — liczba komputerów w grupie
- **Typ** — typ grupy (statyczna lub dynamiczna)
- **Kryteria** (tylko w przypadku grup dynamicznych) — kryteria grupowania
- **Opis** — opis grupy (jeśli określono)

Planów tworzenia kopii zapasowych

Wyświetla listę scentralizowanych planów tworzenia kopii zapasowych powiązanych z grupą i umożliwia realizowanie następujących operacji:

Zadanie	Czynności
Wyświetlanie szczegółów planu tworzenia kopii zapasowych	Kliknij  Szczegóły . W oknie Plany i zadania tworzenia kopii zapasowych zapoznaj się ze wszystkimi informacjami na temat wybranego planu.
Wyświetlanie dziennika planu tworzenia kopii zapasowych	Kliknij  Dziennik . Widok Dziennik przedstawi listę wszystkich wpisów w dzienniku związanych z wybranym planem tworzenia kopii zapasowych.
Uruchamianie planu tworzenia kopii zapasowych	1. Kliknij  Uruchom . 2. Z listy rozwijanej wybierz w ramach planu zadanie, które należy uruchomić. Uruchomienie planu tworzenia kopii zapasowych powoduje natychmiastowe uruchomienie wybranego zadania na komputerach, na których jest wdrożony plan, niezależnie od jego harmonogramu i warunków. Scentralizowanego planu tworzenia kopii zapasowych nie można uruchomić ręcznie, jeśli na co najmniej jednym z komputerów jest uruchomiony agent Acronis Backup & Recovery 10.
Zatrzymywanie planu tworzenia kopii zapasowych	Kliknij  Zatrzymaj . Zatrzymanie wykonywanego planu tworzenia kopii zapasowych powoduje zatrzymanie wszystkich jego zadań na wszystkich komputerach, na których jest on wdrożony. Dlatego wszystkie operacje zadań zostaną przerwane. Scentralizowanego planu tworzenia kopii zapasowych nie można zatrzymać ręcznie, jeśli na co najmniej jednym z komputerów jest uruchomiony agent Acronis Backup & Recovery 10.
Odświeżanie tabeli	Kliknij  Odśwież . Konsola zarządzania zaktualizuje listę istniejących planów tworzenia kopii zapasowych dla grupy komputerów z uwzględnieniem najnowszych informacji. Lista odświeża się automatycznie na podstawie zdarzeń. Mimo to, ze względu na pewne opóźnienie dane z grupy komputerów zarządzanych mogą nie pojawić się natychmiast. Po ręcznym odświeżeniu wyświetlane są najbardziej aktualne dane.

Filtrowanie i sortowanie

Filtrowanie i sortowanie planów i zadań tworzenia kopii zapasowych realizuje się w ten sam sposób, co w przypadku widoku **Plany i zadania tworzenia kopii zapasowych**. Aby uzyskać szczegółowe informacje, zobacz Sortowanie, filtrowanie i konfigurowanie elementów tabeli (s. 26).

11.3.3 Maszyny wirtualne

Maszynami wirtualnymi można zarządzać za pomocą jednej z następujących metod (lub dwóch jednocześnie):

Dodanie maszyny wirtualnej jako komputera fizycznego

Zainstaluj na maszynie wirtualnej komponent Acronis Backup & Recovery 11 Agent for Windows lub Agent for Linux i zarejestruj (s. 330) ją na serwerze zarządzania. Maszyna będzie traktowana jak komputer fizyczny. Pojawi się ona w obszarze **Komputery z agentami**, w grupie **Wszystkie komputery z agentami**.

Ta metoda jest wygodna, gdy:

- maszyna nie znajduje się na serwerze wirtualizacji;
- nie posiadasz licencji wersji Acronis Backup & Recovery 11 Virtual Edition;
- wersja Virtual Edition nie obsługuje tworzenia kopii zapasowych na poziomie hiperwizora dla tego konkretnego programu wirtualizującego;
- musisz pokonać ograniczenia kopii zapasowej na poziomie hiperwizora.

Dodanie maszyny wirtualnej jako maszyny wirtualnej

Na serwerze zarządzania Acronis Backup & Recovery 11 Management Server komputer jest traktowany jako maszyna wirtualna, jeśli można wykonać jego kopię zapasową z hosta wirtualizacji, nie instalując na nim agenta. Umożliwia to wersja Acronis Backup & Recovery 11 Advanced Server Virtual.

Maszynę wirtualną do serwera zarządzania można dodać na kilka sposobów:

- Włącz integrację serwera zarządzania z serwerem vCenter Server.
Rezultat. Maszyny wirtualne zarządzane przez serwer vCenter Server znajdują się w obszarze **Maszyny wirtualne** w grupie **Wszystkie maszyny wirtualne**. Maszyny wyglądają na niezarządzane (są wyszarzone), ale można tworzyć ich kopie zapasowe, jeśli podczas integracji włączono automatyczne wdrażanie agentów.
- Zainstaluj i skonfiguruj komponent Agent for ESX(i) VMware vSphere (Virtual Appliance) lub Agent for ESX(i) VMware vSphere (Windows). Zarejestruj agenta na serwerze zarządzania.
Rezultat. Komputer z agentem (urządzenie wirtualne lub host systemu Windows) pojawi się w obszarze **Komputery z agentami** w grupie **Wszystkie komputery z agentami**. Maszyny wirtualne zarządzane przez agenta znajdują się w obszarze **Maszyny wirtualne** w grupie **Wszystkie maszyny wirtualne**.
- Zainstaluj komponent Agent for Hyper-V na hoście Hyper-V lub na wszystkich węzłach klastra Hyper-V. Zarejestruj agenty na serwerze zarządzania.
Rezultat. Host (węzły) Hyper-V pojawi się w obszarze **Komputery z agentami** w grupie **Wszystkie komputery z agentami**. Maszyny wirtualne zarządzane przez agentów znajdują się w obszarze **Maszyny wirtualne** w grupie **Wszystkie maszyny wirtualne**.

Maszyny wirtualne dodane do serwera zarządzania jako maszyny wirtualne są widoczne w grupie **Maszyny wirtualne** w drzewie **Nawigacja**. Aby uzyskać więcej informacji na temat dostępnych operacji dotyczących tych maszyn, zobacz dokument „Tworzenie kopii zapasowych maszyn wirtualnych”.

11.3.4 Plany i zadania tworzenia kopii zapasowych

Widok **Plany i zadania tworzenia kopii zapasowych** zawiera informacje o ochronie danych na komputerach zarejestrowanych na serwerze zarządzania. Wyświetla on listę scentralizowanych planów tworzenia kopii zapasowych istniejących na serwerze zarządzania, a także zadania serwera zarządzania i węzłów magazynowania.

Aby sprawdzić, czy dane są skutecznie chronione na komputerach, na których wdrożono scentralizowany plan, zapoznaj się z łącznym statusem planu.

Aby sprawdzić, czy scentralizowany plan tworzenia kopii zapasowych jest właśnie wdrażany, usuwany lub aktualizowany, sprawdź stan wdrażania planu. W każdym ze stanów plan tworzenia kopii zapasowych może mieć jeden z następujących statusów: **Błąd**, **Ostrzeżenie** lub **OK**.





W celu śledzenia bieżącego postępu zadania należy sprawdzać jego stan (s. 286). Sprawdzając status (s. 286) zadania, można ustalić jego wynik.





Typowy przepływ roboczy



- Aby w tabeli planów tworzenia kopii zapasowych wyświetlić żądane plany (zadania), skorzystaj z filtrów. Domyślnie w tabeli są wyświetlane wszystkie plany z komputera zarządzanego posortowane według nazwy. Możesz również ukrywać niepotrzebne kolumny i wyświetlać kolumny ukryte. Aby uzyskać więcej informacji, zobacz Sortowanie, filtrowanie i konfigurowanie elementów tabeli (s. 26).
- W tabeli wybierz plan (zadanie) tworzenia kopii zapasowych.
- Aby wykonać czynność dotyczącą wybranego planu (zadania), użyj przycisków na pasku narzędzi. Aby uzyskać szczegółowe informacje, zobacz sekcję Czynności dotyczące scentralizowanych planów i zadań tworzenia kopii zapasowych (s. 341).
- Aby przejrzeć szczegółowe informacje na temat wybranego planu (zadania), skorzystaj z panelu informacyjnego w dolnej części okna. Panel jest domyślnie zwinięty. Aby go rozwinąć, kliknij symbol strzałki (▲). Zawartość panelu jest także dostępna odpowiednio w oknach **Szczegóły planu** (s. 292) i **Szczegóły zadania** (s. 293).

Czynności dotyczące scentralizowanych planów i zadań tworzenia kopii zapasowych

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji dotyczących zadań i scentralizowanych planów tworzenia kopii zapasowych.

Zadanie	Czynności
Utworzenie nowego planu tworzenia kopii zapasowych lub zadania na zarejestrowanym komputerze	<p>Kliknij  Nowy i wybierz jedną z następujących opcji:</p> <ul style="list-style-type: none"> ▪ Plan tworzenia kopii zapasowych (scentralizowany) (s. 315) ▪ Zadanie odzyskiwania (s. 130) ▪ Zadanie sprawdzania poprawności (s. 231) <p>W przypadku tworzenia zadań odzyskiwania lub sprawdzania poprawności należy określić zarejestrowany komputer, na którym będzie uruchamiane wybrane zadanie.</p>
Wyświetlanie szczegółów wybranego planu lub zadania	<p>Kliknij  Wyświetl szczegóły.</p> <p>W oknie Szczegóły planu lub Szczegóły zadania zapoznaj się z wszystkimi informacjami dotyczącymi wybranego planu lub zadania.</p>
Wyświetlanie dziennika planu lub zadania	<p>Kliknij  Wyświetl dziennik.</p> <p>Widok Dziennik (s. 352) przedstawi listę wszystkich wpisów w dzienniku związanych z wybranym planem lub zadaniem.</p>
Uruchamianie planu lub zadania tworzenia kopii zapasowych	<p><u>Plan tworzenia kopii zapasowych</u></p> <ol style="list-style-type: none"> 1. Kliknij  Uruchom. 2. Z listy rozwijanej wybierz w ramach planu zadanie, które należy uruchomić. <p>Uruchomienie planu tworzenia kopii zapasowych powoduje natychmiastowe uruchomienie wybranego zadania na komputerach, na których jest wdrożony plan, niezależnie od jego harmonogramu i warunków.</p> <p>Scentralizowanego planu tworzenia kopii zapasowych nie można uruchomić ręcznie, jeśli na co najmniej jednym z komputerów jest uruchomiony agent Acronis Backup & Recovery 10.</p>

Zadanie	Czynności
	<p><u>Zadanie</u></p> <p>Zadanie zostanie wykonane natychmiast, niezależnie od harmonogramu.</p>
Zatrzymanie wykonywanego planu lub zadania tworzenia kopii zapasowych	<p>Kliknij  Zatrzymaj.</p> <p><u>Scentralizowany plan tworzenia kopii zapasowych</u></p> <p>Zatrzymanie wykonywanego planu tworzenia kopii zapasowych powoduje zatrzymanie wszystkich jego zadań na wszystkich komputerach, na których jest on wdrożony. Dlatego wszystkie operacje zadań zostaną przerwane.</p> <p>Scentralizowanego planu tworzenia kopii zapasowych nie można zatrzymać ręcznie, jeśli na co najmniej jednym z komputerów jest uruchomiony agent Acronis Backup & Recovery 10.</p> <p><u>Zadanie</u></p> <p>Ogólnie rzecz biorąc, zatrzymanie zadania spowoduje przerwanie jego operacji (tworzenia kopii zapasowej, odzyskiwania, sprawdzania poprawności, eksportowania, konwersji itp.) Zadanie przejdzie w stan Bezczynne. Ewentualny harmonogram zadania pozostanie ważny. Aby dokończyć operację, trzeba będzie ponownie uruchomić zadanie.</p>
Edytowanie planu lub zadania	<p>Kliknij  Edytuj.</p> <p><u>Scentralizowany plan tworzenia kopii zapasowych</u></p> <p>Edycję scentralizowanych planów tworzenia kopii zapasowych realizuje się w ten sam sposób, jak ich tworzenie. Po zakończeniu edycji planu serwer zarządzania aktualizuje plan na wszystkich komputerach, na których plan ten został wdrożony.</p> <p><u>Zadanie</u></p> <p>Edycję zadań realizuje się w ten sam sposób, jak ich tworzenie.</p>
Klonowanie planu tworzenia kopii zapasowych	<p>Kliknij  Klonuj.</p> <p>Klon oryginalnego planu tworzenia kopii zapasowych zostanie utworzony z domyślną nazwą „Klon <oryginalna_nazwa_planu>”. Sklonowany plan zostanie od razu wyłączony, aby nie działał równocześnie z planem oryginalnym. Ustawienia sklonowanego planu można zmienić przed jego włączeniem.</p>
Włączanie planu	<p>Kliknij  Włącz.</p> <p>Wcześniej wyłączony plan tworzenia kopii zapasowych będzie uruchamiany ponownie zgodnie z harmonogramem.</p>
Wyłączanie planu	<p>Kliknij  Wyłącz.</p> <p>Plan tworzenia kopii zapasowych nie będzie uruchamiany zgodnie z harmonogramem. Można je jednak uruchamiać ręcznie. Po ręcznym uruchomieniu plan pozostanie w dalszym ciągu wyłączony. Jeśli ponownie włączysz plan, będzie on uruchamiany jak zwykle.</p>
Eksportowanie planu	<p>Kliknij  Eksportuj.</p> <p>Określ ścieżkę i nazwę pliku wynikowego. Aby uzyskać więcej informacji, zobacz Eksportowanie oraz importowanie planów tworzenia kopii zapasowych (s. 287).</p>

Zadanie	Czynności
Importowanie planu	<p>Kliknij  Importuj.</p> <p>Określ ścieżkę i nazwę pliku zawierającego wcześniej wyeksportowany plan. Aby uzyskać więcej informacji, zobacz Eksportowanie oraz importowanie planów tworzenia kopii zapasowych (s. 287).</p>
Usuwanie planu lub zadania	<p>Kliknij  Usuń.</p> <p><u>Scentralizowany plan tworzenia kopii zapasowych</u></p> <p>Wskutek tego scentralizowany plan tworzenia kopii zapasowych zostanie usunięty z serwera zarządzania i komputerów, na których był wdrożony. Jeśli komputer znajduje się w danym momencie w trybie offline, plan zostanie usunięty po jego ponownym przejściu do trybu online.</p> <p><u>Zadanie</u></p> <p>Wskutek tego zadanie zostanie usunięte z serwera zarządzania. Wbudowanych zadań kompaktowania węzłów magazynowania nie można usunąć.</p>

11.3.5 Węzły magazynowania

Węzeł magazynowania Acronis Backup & Recovery 11 Storage Node umożliwia optymalizację korzystania z różnych zasobów potrzebnych do ochrony danych przedsiębiorstwa. Cel ten osiąga się w drodze organizowania skarbów zarządzanych służących jako odrębne magazyny archiwów kopii zapasowych przedsiębiorstwa.

Węzły magazynowania są widoczne w widoku **Węzły magazynowania** po ich instalacji i rejestracji na serwerze zarządzania. Aby uzyskać więcej informacji na temat operacji na węzłach magazynowania, zobacz „Węzły magazynowania” (s. 212).

11.3.6 Licencje

Widok **Licencje** umożliwia zarządzanie licencjami przechowywanymi na serwerze Acronis License Server. Serwer licencji można zintegrować z serwerem Acronis Backup & Recovery 11 Management Server lub zainstalować jako osobny komponent.

Dostęp do widoku Licencje

Aby uzyskać dostęp do widoku **Licencje** po podłączeniu do serwera zarządzania, kliknij **Licencje** w panelu **Nawigacja**.

Aby połączyć się bezpośrednio z serwerem licencji:

1. Z menu konsoli **Narzędzia** wybierz **Zarządzaj licencjami**.
2. Określ nazwę lub adres IP komputera z serwerem licencji.
3. Kliknij **OK**. Otworzy się ten sam widok **Licencje**.

Wyświetlanie informacji o licencjach

W widoku **Licencje** są wyświetlane wszystkie klucze licencyjne zapisane na serwerze licencji. Są one pogrupowane według produktów. Jeden klucz licencyjny może zawierać wiele licencji.

Po kliknięciu prawym przyciskiem myszy paska nagłówek kolumn można wybrać informacje do wyświetlenia: klucz licencyjny, datę wygaśnięcia, datę importowania oraz całkowitą liczbę kluczy licencyjnych, a także liczbę dostępnych (tzn. wolnych) i używanych kluczy.

Aby wyświetlić informacje o określonym kluczu licencyjnym, rozwiń żądany produkt, a następnie klucz. Aby uzyskać informacje na temat komputerów używających licencji, kliknij **Pokaż komputery używające tej licencji**.

Dodawanie licencji

Aby móc dodawać licencje, dodaj je najpierw do serwera licencji.

Aby dodać licencje

1. Kliknij **Dodaj licencję**.
2. W oknie **Określ licencje do dodania** wpisz klucze licencyjne lub zaimportuj je z pliku. Aby zaimportować licencje z pliku .txt, .eml lub .xml, kliknij **Importuj klucze z pliku** i określ plik zawierający listę kluczy licencyjnych. Możesz określić kolejno kilka plików lub wpisać klucze licencyjne ręcznie.
3. Kliknij **OK**.

Zmianie serwera licencji używanego przez serwer zarządzania

Domyślnie serwer zarządzania korzysta ze zintegrowanego serwera licencji. Można go zmusić do korzystania z innego serwera licencji. Jeśli masz już osobny serwer licencji, funkcja ta ułatwia migrację serwera licencji na nowy sprzęt.

Przed zmianą serwera licencji należy wyeksportować (s. 344) licencje ze starego serwera licencji i dodać (s. 344) je do nowego.

Aby zmienić serwer licencji

1. Podłącz konsolę do serwera zarządzania.
2. W panelu **Nawigacja** kliknij **Licencje**.
3. W menu **Czynności** wybierz **Zmień serwer licencji**.
4. Określ nazwę lub adres IP komputera z serwerem licencji.
5. Kliknij **OK**.

Po zmianie serwera licencji serwer zarządzania wdroży na zarejestrowanych komputerach adres IP nowego serwera licencji, po czym zaczną one korzystać z tego nowego serwera.

Eksportowanie licencji

Przed zmianą serwera licencji wyeksportuj licencje z serwera, który chcesz zmienić (s. 344). Wszystkie licencje zostaną zapisane w pliku .xml. Później możesz zaimportować (s. 344) je na nowy serwer licencji.

Aby wyeksportować licencje

1. Kliknij **Eksportuj licencje do pliku XML**.
2. Określ lokalizację docelową pliku (oraz opcjonalnie jego nazwę).
3. Kliknij **OK**, aby zapisać plik.

Usuwanie licencji

Aby całkowicie usunąć licencję z serwera Acronis License Server, wybierz ją na liście dostępnych licencji i na pasku narzędzi kliknij **Usuń licencję**. Aby usunąć używaną licencję, należy ją najpierw odwołać (s. 345).

Odwoływanie licencji

Odwołanie pozwala ponownie udostępnić używane licencje. Może być konieczne w następujących przypadkach:

- Komponent wymagający licencji (na przykład agent) jest odinstalowywany z komputera.
Licencję należy odwołać z komputera przed lub po jego odinstalowaniu.
- Komputer zarządzany zostaje trwale wycofany z eksploatacji.
Licencję należy odwołać z komputera przed lub po wycofaniu go z eksploatacji.

Upewnij się, że odwołanie i późniejsze ponowne użycie licencji nie narusza umowy licencyjnej ani innych wymogów prawnych.

Aby odwołać licencję:

Rozwiń żądany produkt, a następnie jego klucz.

- Jeśli z klucza licencyjnego korzysta pojedynczy komputer, na pasku narzędzi kliknij **Odwołaj licencję**.
- Jeśli z klucza licencyjnego korzysta wiele komputerów, kliknij **Pokaż komputery używające tej licencji**. W otwartym oknie wybierz host, z którego chcesz odwołać licencję (zobacz kolumnę **Nazwa hosta**), i kliknij **Odwołaj licencję**.

Korzystanie z narzędzia Acronis License Server Management Tool

Plik LicenseServerCmdLine.exe znajduje się w folderze instalacyjnym serwera licencji. Domyślnie jest to folder \Program Files\Acronis\LicenseServer.

W narzędziu LicenseServerCmdLine.exe używana jest następująca składnia:

```
LicenseServerCmdLine <polecenie> <parametr1> <parametr2>
```

Polecenie LicenseServerCmdLine.exe obsługuje następujące parametry:

```
--status <adres IP lub nazwa hosta>
```

Wyświetla całkowitą liczbę licencji oraz liczbę licencji dostępnych dla każdego programu firmy Acronis.

```
--import <adres IP lub nazwa hosta> <klucz licencji>
```

Dodaje nowy klucz licencyjny do określonego serwera licencji. Można określić wiele kluczy licencyjnych rozdzielonych spacjami.

```
--import-file <adres IP lub nazwa hosta> <nazwa pliku>
```

Importuje klucze licencyjne z pliku .txt lub .eml.

```
--help
```

Wyświetla pomoc.

11.3.7 Raporty

Dzięki raportom administrator serwera zarządzania może poznać dokładne, uporządkowane informacje dotyczące operacji związanych z ochroną danych w korporacji. Raporty mogą być instrumentem do realizacji dokładnej analizy całej infrastruktury kopii zapasowych w sieci korporacyjnej.

Raporty są tworzone przez serwer zarządzania na podstawie statystyk i dzienników zebranych z zarejestrowanych komputerów i przechowywanych w specjalnych bazach danych.

Szablony raportów

Raporty są generowane na podstawie szablonów raportów. Szablony służą do definicji informacji uwzględnianych w raporcie i sposobu ich prezentacji.

Serwer zarządzania Acronis Backup & Recovery 11 Management Server oferuje następujące typy szablonów raportów:

- Zarejestrowane komputery.
- Lokalne i scentralizowane plany tworzenia kopii zapasowych istniejące na zarejestrowanych komputerach.
- Lokalne i scentralizowane zadania istniejące na zarejestrowanych komputerach.
- Archiwa i kopie zapasowe przechowywane w centralnych skarbcach zarządzanych.
- Statystyki centralnego skarbcza zarządzanego.
- Historia działań dotyczących zadań.

Raporty o komputerach, planach tworzenia kopii zapasowych, zadaniach oraz archiwach i kopiach zapasowych są aktualizowane na bieżąco.

Raporty o statystykach skarbców i działaniach dotyczących zadań są tworzone dla określonych przedziałów czasu i przedstawiają odpowiadające im informacje historyczne. Przedziały mogą wynosić od kilku dni do kilku lat, w zależności od ilości danych przechowywanych w bazach.

Konfigurowanie i generowanie raportów

Istnieją dwa typy szablonów raportów: niestandardowe i wstępnie zdefiniowane.

W szablonie niestandardowym można za pomocą filtrów określić pozycje uwzględniane w raporcie oraz sposoby ich grupowania i sortowania. Aby skonfigurować raport, w widoku **Raporty** wybierz szablon raportu, kliknij **Konfiguruj** na pasku narzędzi, a następnie ustaw **Filtry** i **Widok raportu**. Kliknij **OK**, aby wygenerować raport.

Wstępnie zdefiniowany szablon raportu pozwala na utworzenie raportu za pomocą jednego kliknięcia myszą. Aby rozpocząć generowanie raportu, wybierz szablon raportu w widoku **Raporty** i kliknij **Wygeneruj** na pasku narzędzi.

Raport będzie zawierać informacje wybrane, pogrupowane i posortowane zgodnie z ustawieniami szablonu. Wybierz, czy chcesz przejrzeć raport w domyślnej przeglądarce czy zapisać go w pliku.xml. Raport przeglądany jest wyświetlany w oddzielnym interaktywnym oknie, które umożliwia rozwijanie i zwijanie tabel. Do otwarcia zapisanego pliku .xml użyj aplikacji Microsoft Excel lub Microsoft Access.

Raporty o komputerach

Za pomocą tego widoku można utworzyć raport o komputerach, które nie są zarejestrowane na serwerze zarządzania. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz komputery, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko te komputery, które spełniają wszystkie kryteria,

- **Komputery** — lista komputerów. Wybierz komputery z agentami lub maszyny wirtualne. [Opcjonalnie] Kliknij **Wybierz**, aby wybrać określone komputery lub grupy komputerów.
- **Status** — statusy komputerów: **OK**, **Ostrzeżenie** lub **Błąd**.
- **Ostatnie połączenie** (tylko komputery z agentami) — okres ostatniego połączenia między komputerami i serwerem zarządzania.

- **Ostatnia pomyślnie utworzona kopia zapasowa** — okres ukończenia ostatniej pomyślnie utworzonej kopii zapasowej na każdym z komputerów.
- **Następna kopia zapasowa** — okres uruchomienia następnej zaplanowanej operacji tworzenia kopii zapasowej na każdym z komputerów.
- **System operacyjny** — systemy operacyjne działające na komputerach.
- **Adres IP** (tylko komputery z agentami) — zakres ostatnio uzyskanych adresów IP komputerów.
- **Dostępność** (tylko komputery z agentami) — typy dostępności komputerów: **Online** lub **Offline**.

Przy domyślnych ustawieniach filtra raport obejmie wszystkie komputery z agentami.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.
- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raport o planach tworzenia kopii zapasowych

W tym widoku można utworzyć raporty o istniejących na zarejestrowanych komputerach planach tworzenia kopii zapasowych. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz plany tworzenia kopii zapasowych, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko te zasady, które spełniają wszystkie kryteria,

- **Początek** — typy pochodzenia planów tworzenia kopii zapasowych: **Lokalny** lub **Centralny**.
- **Komputery** — lista komputerów, na których istnieją plany tworzenia kopii zapasowych.
- **Typ danych uwzględnionych w kopii zapasowej** — typy danych uwzględnionych w kopii zapasowej — **Komputery/Dyski/Woluminy** lub **Pliki**.
- **Stan wdrażania** — stan wdrażania planów tworzenia kopii zapasowych, na przykład **Odwóływanie**.
- **Stan wykonania** — stany wykonania planów tworzenia kopii zapasowych, na przykład **Uruchomione**.
- **Status** — statusy planów tworzenia kopii zapasowych: **OK**, **Ostrzeżenie** lub **Błąd**.
- **Godzina ostatniego zakończenia** — moment ukończenia ostatniego zadania planu tworzenia kopii zapasowych.
- **Harmonogram** — typy harmonogramów planów tworzenia kopii zapasowych: **Ręczne** lub **Zaplanowane**. Harmonogram ręczny oznacza, że plan tworzenia kopii zapasowych zostanie uruchomiony tylko po jego ręcznym wywołaniu.
- **Właściciel** — lista użytkowników, którzy utworzyli plany tworzenia kopii zapasowych.

Przy domyślnych ustawieniach filtra raport obejmie wszystkie plany tworzenia kopii zapasowych ze wszystkich komputerów.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.

- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raport o zadaniach

W tym widoku można utworzyć raport o zadaniach uruchomionych na zarejestrowanych komputerach. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz zadania, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko zadania spełniające wszystkie kryteria filtru.

- **Początek** — typy pochodzenia zadań: **Centralny**, **Lokalny** i/lub **Lokalny bez planu tworzenia kopii zapasowych**. Zadanie scentralizowane należy do scentralizowanego planu tworzenia kopii zapasowych. Zadanie lokalne może nie należeć do planu tworzenia kopii zapasowych (na przykład zadanie odzyskiwania).
- **Plany tworzenia kopii zapasowych** (tylko zadania scentralizowane) — plany tworzenia kopii zapasowych, na których są oparte zadania.
- **Komputery** — lista komputerów, na których istnieją zadania.
- **Typ** — typy zadań, na przykład zadania tworzenia kopii zapasowych.
- **Stan wykonania** — stany wykonania zadań, na przykład **Uruchomione**.
- **Ostatni wynik** — ostatnie wyniki zadań: **Wykonane pomyślnie**, **Wykonane pomyślnie z ostrzeżeniami**, **Zakończone niepowodzeniem**, **Zatrzymane** lub „-” (jeszcze bez wyniku).
- **Harmonogram** — typy harmonogramów zadań: **Ręczne** lub **Zaplanowane**. Harmonogram ręczny oznacza, że zadanie zostanie uruchomione tylko po jego ręcznym wywołaniu.
- **Właściciel** — lista użytkowników, którzy utworzyli zadania.
- **Czas trwania** — długość ostatniego wykonywania poszczególnych zadań.

Przy domyślnych ustawieniach filtra raport obejmie wszystkie zadania ze wszystkich komputerów.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.
- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raport o archiwach i kopiach zapasowych

W tym widoku można wygenerować raport o archiwach przechowywanych w zarządzanych skarbonach centralnych. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz archiwa, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko archiwa spełniające wszystkie kryteria filtru.

- **Skarbonce** — lista zarządzanych skarbonców centralnych, w których przechowywane są archiwa.
- **Komputery** — lista zarejestrowanych komputerów, z których utworzono archiwa.
- **Typ** — typy archiwów: na poziomie dysku i/lub na poziomie pliku.
- **Właściciel** — lista użytkowników, którzy utworzyli archiwa.

- **Godzina utworzenia** — okres utworzenia ostatniej kopii zapasowej w każdym z archiwów.
- **Zajęte miejsce** — limity miejsca zajmowanego przez każde z archiwów.
- **Dane uwzględnione w kopii zapasowej** — limity łącznego rozmiaru danych przechowywanych aktualnie w każdym z archiwów. Rozmiar ten może odbiegać od zajętego miejsca z powodu kompresji lub deduplikacji.
- **Liczba kopii zapasowych** — limit liczby kopii zapasowych znajdujących się w każdym archiwum.

Przy domyślnych ustawieniach filtru raport obejmie wszystkie archiwa przechowywane w zarządzanych skarbcach centralnych.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.
- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raporty o statystykach skarbców

W tym widoku można wygenerować raport o wykorzystaniu centralnych skarbców zarządzanych, które są obecnie dodane do serwera zarządzania. Raport składa się z przynajmniej jednej tabeli i diagramu.

Zakres raportu

W sekcji **Zakres raportu** wybierz przedział czasu, dla którego chcesz wygenerować raport. W raporcie wyświetlany jest stan wybranych skarbców o podanej porze każdego dnia okresu uwzględnionego w raporcie.

Filtry

W sekcji **Filtry** wybierz centralne skarbcze zarządzane, które chcesz uwzględnić w raporcie, oraz określ, czy chcesz utworzyć podsumowanie dotyczące wszystkich wybranych skarbców.

Podsumowanie przedstawia łączną ilość wolnego i zajętego miejsca, łączną ilość danych w kopiach zapasowych, łączną liczbę archiwów i kopii zapasowych oraz średnie wartości wskaźników w wybranych skarbcach.

Przy domyślnych ustawieniach filtru raport obejmie informacje o wszystkich centralnych skarbcach zarządzanych oraz podsumowanie.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ wyświetlane kolumny tabeli i ich kolejność.
- Wybierz diagramy do uwzględnienia w raporcie. Diagramy przedstawiają poziom wykorzystania miejsca w skarbcach.

Raport o czynnościach zadań

W tym widoku można utworzyć raport o zadaniach istniejących na zarejestrowanych komputerach w wybranym okresie. Raport składa się z przynajmniej jednego diagramu. Jeden diagram odpowiada jednemu komputerowi.

Diagramy przedstawiają, ile razy zadanie zostało pomyślnie wykonane danego dnia z jednym z następujących rezultatów: „Wykonane pomyślnie”, „Wykonane pomyślnie z ostrzeżeniami” i „Zakończone niepowodzeniem”.

Zakres raportu

W sekcji **Zakres raportu** wybierz przedział czasu, dla którego chcesz wygenerować raport.

Filtry

W sekcji **Filtry** wybierz zadania, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko zadania spełniające wszystkie kryteria filtru.

- **Początek** — typy pochodzenia zadań: **Centralny**, **Lokalny** i/lub **Lokalny bez planu tworzenia kopii zapasowych**. Zadanie scentralizowane należy do scentralizowanego planu tworzenia kopii zapasowych. Zadanie lokalne może nie należeć do planu tworzenia kopii zapasowych (na przykład zadanie odzyskiwania).
- **Plany tworzenia kopii zapasowych** (tylko zadania scentralizowane) — plany tworzenia kopii zapasowych, na których są oparte zadania. Ustawienie domyślne oznacza wszystkie plany tworzenia kopii zapasowych, które kiedykolwiek istniały w okresie uwzględnionym w raporcie.
- **Komputery** — lista komputerów, na których istnieją zadania.
- **Typ** — typy zadań, na przykład zadania tworzenia kopii zapasowych.
- **Właściciel** — lista użytkowników, którzy utworzyli zadania.

Przy domyślnych ustawieniach filtra w raporcie zostaną umieszczone wszystkie zadania, które istniały na zarejestrowanych komputerach kiedykolwiek w danym okresie.

Wybór kolumn

W oknie **Wybór kolumn** można wybrać kolumny do uwzględnienia w raporcie i określić ich kolejność.

Kolumny zawarte w tabelach raportu (od lewej do prawej strony) będą zgodne z listą w sekcji **Wyświetl w raporcie**. Najwyższa kolumna na liście znajdzie się po lewej stronie raportu.

Podczas wybierania wyświetlanych kolumn przyciski strzałek w lewo i w prawo służą odpowiednio do uwzględniania i wykluczania kolumn, a przyciski strzałek w górę i w dół — do zmiany ich kolejności.

Niektórych kolumn — na przykład **Nazwa komputera** w raporcie o komputerach — nie można wykluczyć z listy ani przesunąć w górę lub w dół.

Widok raportu

Aby przeglądarka internetowa mogła prawidłowo wyświetlać daty i inne informacje z generowanych raportów, włącz obsługę zawartości aktywnej (JavaScript). Możesz ją włączyć tylko dla obecnie wyświetlanej strony lub na stałe. Aby umożliwić tymczasową obsługę zawartości aktywnej w przeglądarce Internet Explorer, kliknij pasek Informacje wyświetlany u góry strony i kliknij **Zezwalaj na zablokowaną zawartość**.

Aby trwale włączyć zawartość aktywną

W przeglądarce Internet Explorer

1. W menu **Narzędzia** kliknij **Opcje internetowe**, a następnie kliknij kartę **Zaawansowane**.
2. W sekcji **Zabezpieczenia** zaznacz pole wyboru **Zezwalaj zawartości aktywnej na działanie w plikach na moim komputerze**.
3. Kliknij **OK**.

W przeglądarce Mozilla Firefox

1. W menu **Opcje** kliknij **Treść**.
2. Sprawdź, czy pole wyboru **Włącz obsługę języka JavaScript** jest zaznaczone.
3. Kliknij **OK**.

11.3.8 Alerty

Alert to komunikat ostrzegawczy informujący o rzeczywistych lub potencjalnych problemach. Widok **Alerty** pozwala na błyskawiczną identyfikację i rozwiązywanie problemów, umożliwiając monitorowanie bieżących alertów i podgląd ich historii.

Alerty aktywne i nieaktywne

Alert może znajdować się w stanie aktywnym lub nieaktywnym. Stan aktywny oznacza, że problem, który go wywołał, w dalszym ciągu istnieje. Alert staje się nieaktywny, gdy problem, który go wywołał, został ręcznie lub samoistnie rozwiązany.

Uwaga: *Jeden rodzaj alertu pozostaje zawsze aktywny: „Nie utworzono kopii zapasowej”. Wiąże się to z faktem, iż nawet po rozwiązaniu przyczyny alertu i pomyślnym utworzeniu kolejnych kopii zapasowych problem dotyczący nieutworzenia kopii zapasowej w dalszym ciągu istnieje.*

Naprawianie błędów, które wywołały alerty

Aby znaleźć i naprawić problem, który wywołał alert, kliknij **Napraw problem**. Nastąpi przeniesienie do odpowiedniego widoku, gdzie można przeanalizować problem i podjąć niezbędne kroki naprawcze.

Opcjonalnie można kliknąć **Wyświetl szczegóły** i uzyskać pełniejsze informacje na temat zaznaczonego alertu.

Akceptowanie alertów

Domyślnie w tabeli **Bieżące alerty** znajdują się zarówno aktywne, jak i nieaktywne alerty do czasu ich zaakceptowania. Aby zaakceptować alert, zaznacz go i kliknij **Zaakceptuj**. Przez zaakceptowanie alertu przyjmujesz do wiadomości fakt jego wystąpienia i zgadzasz się na przyjęcie za niego odpowiedzialności. Zaakceptowane alerty są przenoszone do tabeli **Zaakceptowane alerty** z niezmienioną informacją o ich stanie.

W tabeli **Zaakceptowane alerty** jest przechowywana historia zaakceptowanych alertów. Umożliwia ona ustalenie osoby, która zaakceptowała dany alert, oraz daty i godziny tego zdarzenia. Zaakceptowane alerty w obu stanach można usuwać z tabeli ręcznie — za pomocą przycisków **Usuń** oraz **Usuń wszystkie**, lub automatycznie (zobacz „Konfigurowanie alertów” w dalszej części tej sekcji).

Aby wyeksportować pełną zawartość tabeli do pliku *.txt lub *.csv, kliknij **Zapisz wszystko w pliku**.

Widok Alerty na serwerze zarządzania

Po podłączeniu konsoli do serwera zarządzania widok **Alerty** przedstawia listę alertów zebranych zarówno z zarejestrowanych komputerów, jak i z serwera zarządzania.

Alerty zebrane z zarejestrowanych komputerów:

- pojawiają się w widoku **Alerty** niezależnie od ich widoczności na tych komputerach;
- osobno zaakceptowane zarówno na serwerze zarządzania, jak i na zarejestrowanych komputerach.

Podobne alerty zebrane z kilku komputerów są łączone w postaci pojedynczego alertu grupowego. Kolumna **Komputer** alertów grupowych przyjmuje postać **Wiele (X)**, gdzie **X** to liczba zarejestrowanych komputerów zgłaszających taki alert. Po dezaktywacji pojedynczego aktywnego alertu w grupie zostaje on przeniesiony do nowej lub istniejącej grupy nieaktywnej. Liczba komputerów, których dotyczy alert (**X**), zostanie zmniejszona w przypadku aktywnego alertu grupowego i odpowiednio zwiększona w przypadku nieaktywnego alertu grupowego.

Aby uzyskać informacje o komputerach związanych z określonym alertem grupowym, kliknij **Wyświetl szczegóły**.

Konfigurowanie alertów

Do konfigurowania alertów służą następujące opcje dostępne w górnej części widoku **Alerty**:

- **Pokaż/ukryj alerty** (s. 29) — określenie typów alertów wyświetlanych w widoku **Alerty**.
- **Powiadomienia** (s. 357) — konfiguracja powiadomień e-mail o zgłaszanych alertach.
- **Ustawienia** (s. 355) — możliwość określenia, czy nieaktywne alerty mają być automatycznie przenoszone do tabeli **Zaakceptowane alerty**, oraz wskazania okresu przechowywania zaakceptowanych alertów w tabeli **Zaakceptowane alerty**.

11.3.9 Dziennik

W scentralizowanym dzienniku zdarzeń jest przechowywana historia operacji wykonywanych przez serwer zarządzania, węzły magazynowania i zarejestrowane komputery.

Aby wyświetlić zwykłą listę wpisów dziennika, wybierz **Zdarzenia** z listy rozwijanej **Wyświetlaj**. Aby wyświetlić wpisy dziennika pogrupowane według działań, wybierz **Działania**. Szczegółowe informacje na temat wybranego wpisu dziennika lub działania są wyświetlane w panelu **Informacje** w dolnej części widoku **Dziennik**.

Aby wyświetlić żądane działania i wpisy dziennika w tabeli, skorzystaj z filtrów. Możesz również ukrywać niepotrzebne kolumny i wyświetlać kolumny ukryte. Aby uzyskać szczegółowe informacje, zobacz Sortowanie, filtrowanie i konfigurowanie elementów tabeli (s. 26). Po wybraniu elementów w innych widokach administracyjnych (**Pulpit nawigacyjny**, **Komputery z agentami**, **Plany i zadania tworzenia kopii zapasowych**) można wyświetlić widok **Dziennik** zawierający odfiltrowane wpisy dotyczące tych elementów.







Wybierz żądane działanie lub wpis, aby wykonać związaną z nim czynność. Aby uzyskać szczegółowe informacje, zobacz Czynności dotyczące wpisów dziennika (s. 352) oraz Szczegóły wpisu dziennika (s. 353).

Czynności dotyczące wpisów dziennika (scentralizowanego)

Wszystkie operacje opisane poniżej wykonuje się przez kliknięcie odpowiednich elementów na **pasku narzędzi** dziennika. Operacje te można również wykonać za pomocą menu kontekstowego (klikając prawym przyciskiem myszy wpis dziennika lub działanie)

Poniżej przedstawiono wytyczne dotyczące wykonywania czynności związanych z wpisami dziennika.

Zadanie	Czynności
Wybieranie pojedynczego działania	Z listy rozwijanej Wyświetlaj wybierz Działania i kliknij działanie. Panel Informacje będzie zawierał wpisy dziennika dotyczące wybranego działania.
Wybieranie pojedynczego	Kliknij wpis.

wpisu dziennika	
Wybieranie wielu wpisów dziennika	<ul style="list-style-type: none"> ▪ <i>Niesqsiadujące</i>: przytrzymaj klawisz CTRL i pojedynczo klikaj żądane wpisy dziennika. ▪ <i>Sqsiadujące</i>: wybierz jeden wpis dziennika, a następnie przytrzymaj klawisz SHIFT i kliknij inny wpis dziennika. Wszystkie wpisy dziennika między pierwszym a ostatnim również zostaną wybrane.
Wyświetlanie szczegółów wpisu dziennika	<ol style="list-style-type: none"> 1. Wybierz wpis dziennika. 2. Wykonaj jedną z następujących czynności: <ul style="list-style-type: none"> ▪ Kliknij dwukrotnie zaznaczenie. ▪ Kliknij  Szczegóły. <p>Zostaną wyświetlone szczegóły wpisu dziennika. Aby poznać szczegółowe informacje dotyczące działań związanych z wpisami dziennika, zobacz Szczegóły wpisu dziennika (s. 353).</p>
Zapisywanie wybranych wpisów dziennika w pliku	<ol style="list-style-type: none"> 1. Wyświetl Działania i wybierz działania lub wyświetl Zdarzenia i wybierz wpisy dziennika. 2. Kliknij  Zapisz zaznaczone w pliku. 3. W otwartym oknie określ ścieżkę i nazwę pliku. <p>W określonym pliku zostaną zapisane wszystkie wpisy dziennika dotyczące wybranych działań lub wybrane wpisy dziennika.</p>
Zapisywanie wszystkich wpisów dziennika w pliku	<ol style="list-style-type: none"> 1. Upewnij się, że nie są ustawione żadne filtry. 2. Kliknij  Zapisz wszystko w pliku. 3. W otwartym oknie określ ścieżkę i nazwę pliku. W określonym pliku zostaną zapisane wszystkie wpisy dziennika.
Zapisywanie wszystkich odfiltrowanych wpisów dziennika w pliku	<ol style="list-style-type: none"> 1. Ustaw filtry tak, aby uzyskać listę wpisów dziennika spełniających kryteria filtrowania. 2. Kliknij  Zapisz wszystko w pliku. 3. W otwartym oknie określ ścieżkę i nazwę pliku. <p>W określonym pliku zostaną zapisane wszystkie wpisy dziennika z listy.</p>
Usuwanie wszystkich wpisów dziennika	<p>Kliknij  Wyczyść dziennik.</p> <p>Wszystkie wpisy dziennika zostaną usunięte z dziennika i zostanie utworzony nowy wpis dziennika. Będzie on zawierał informację o tym, kto i kiedy usunął wpisy dziennika.</p>
Konfigurowanie poziomu rejestrowania	<p>Kliknij  Konfiguruj poziom rejestrowania.</p> <p>W oknie Poziom dziennik (s. 358) określ typy zdarzeń pochodzących z zarejestrowanych komputerów, które chcesz gromadzić w scentralizowanym dzienniku.</p>

Szczegóły wpisu scentralizowanego dziennika

W tym miejscu wyświetlane są szczegółowe informacje dotyczące wybranego wpisu dziennika. Informacje te można skopiować do schowka.

Aby wyświetlić szczegółowe informacje na temat następnego lub poprzedniego wpisu dziennika, kliknij odpowiednio przycisk strzałki w dół lub w górę.

Aby skopiować szczegóły, kliknij przycisk **Kopiuj do schowka**.

Pola danych wpisu dziennika

Wpis dziennika zawiera następujące pola danych:

- **Typ** — typ zdarzenia (Błąd, Ostrzeżenie, Informacja).
- **Data i godzina** — data i godzina wystąpienia zdarzenia.
- **Plan tworzenia kopii zapasowych** — plan tworzenia kopii zapasowych, z którym związane jest zdarzenie (jeśli dotyczy).
- **Zadanie** — zadanie, z którym związane jest zdarzenie (jeśli dotyczy).
- **Komputer** — nazwa komputera, na którym wystąpiło zdarzenie (jeśli dotyczy). Pole jest widoczne tylko w dzienniku scentralizowanym.
- **Kod** — wartość pusta lub kod błędu programu, jeśli typem zdarzenia jest błąd. Kod błędu to liczba całkowita, która może posłużyć działowi pomocy technicznej firmy Acronis do rozwiązania problemu.
- **Moduł** — wartość pusta lub numer modułu programu, w którym wystąpił błąd. Jest to liczba całkowita, która może posłużyć działowi pomocy technicznej firmy Acronis do rozwiązania problemu.
- **Właściciel** — nazwa użytkownika będącego właścicielem (s. 32) planu tworzenia kopii zapasowych.
- **Komunikat** — tekstowy opis zdarzenia.

11.3.10 Opcje serwera zarządzania

Opcje serwera zarządzania umożliwiają dostosowanie zachowania serwera Acronis Backup & Recovery 11 Management Server.

Aby uzyskać dostęp do opcji serwera zarządzania, podłącz konsolę do serwera, a następnie wybierz polecenia **Opcje > Opcje serwera zarządzania** z górnego menu.

Acronis WOL Proxy

Ta opcja działa w połączeniu z zaawansowanym ustawieniem harmonogramu **Użyj Wake-on-LAN** (s. 85). Użyj tej opcji, jeśli serwer zarządzania musi obudzić komputery zlokalizowane w innej podsieci, których kopia zapasowa ma być wykonana.

Gdy zaplanowana operacja ma się zacząć, serwer zarządzania wysyła specjalne pakiety służące do obudzenia odpowiednich komputerów. (Specjalny pakiet zawiera 16 ciągłych kopii adresu MAC karty sieciowej odbiorcy). Zainstalowany w innej podsieci program Acronis WOL Proxy przenosi pakiety do komputerów znajdujących się w tej samej podsieci.

Ustawienie wstępne: **Wyłączone**.

Aby włączyć tę opcję:

1. Zainstaluj program Acronis WOL Proxy na dowolnym serwerze w podsieci, do której należą także budzone komputery. Serwer musi być dostępny w trybie ciągłym. Przy wielu podsieciach zainstaluj program Acronis WOL Proxy w każdej podsieci, w której chcesz używać funkcji Wake-On-LAN.
2. Włącz program **Acronis WOL Proxy** w **opcjach serwera zarządzania** w następujący sposób:
 - a. Zaznacz pole wyboru **Użyj następujących proxy**.

- b. Kliknij **Dodaj** i wprowadź nazwę lub adres IP komputera z zainstalowanym programem Acronis WOL Proxy. Podaj poświadczenia dla danego komputera.
 - c. Powtórz ten krok, jeśli zainstalowano kilka programów Acronis WOL Proxies.
3. Podczas planowania scentralizowanego planu tworzenia kopii zapasowych włącz ustawienie **Użyj Wake-on-LAN**.

Istnieje także możliwość usunięcia z listy serwerów proxy. Pamiętaj o tym, że każda zmiana tej opcji ma wpływ na cały serwer zarządzania. Po usunięciu serwera proxy z listy funkcja Wake-On-LAN w odpowiedniej podsieci zostanie wyłączona we wszystkich scentralizowanych planach tworzenia kopii zapasowych, w tym także w już wdrożonych planach.

Alerty

Zarządzanie alertami

Usuwanie z kategorii „Zaakceptowane alerty” elementy starsze niż

Ta opcja pozwala określić, czy zaakceptowane alerty mają być usuwane z tabeli **Zaakceptowane alerty**.

Ustawienie wstępne: **Wyłączone**.

Włączenie opcji umożliwia określenie okresu przechowywania zaakceptowanych alertów. Zaakceptowane alerty starsze niż wskazany okres będą automatycznie usuwane z tabeli.

Automatycznie przenosić nieaktywne alerty do kategorii „Zaakceptowane alerty”

Opcja ta pozwala określić, czy wszystkie alerty, które stają się nieaktywne, mają być automatycznie akceptowane i przenoszone do tabeli **Zaakceptowane alerty**.

Ustawienie wstępne: **Wyłączone**.

Włączenie opcji umożliwia określenie typów alertów, do których ma ona mieć zastosowanie.

Alerty związane z czasem

Ostatnia kopia zapasowa

Ta opcja jest uwzględniana, gdy konsola jest połączona z komputerem zarządzanym (s. 380) lub serwerem zarządzania (s. 384).

Określa ona, czy ma być wyświetlany alert w przypadku, gdy na danym komputerze od pewnego czasu nie została utworzona kopia zapasowa. Można określić czas, który jest krytyczny dla użytkownika.

Ustawienie wstępne: alert w przypadku, gdy ostatnia kopia zapasowa na komputerze została pomyślnie utworzona ponad **5 dni** temu.

Alert jest wyświetlany w sekcji **Alerty** na **Pulpicie nawigacyjnym**. Gdy konsola jest połączona z serwerem zarządzania, to ustawienie określa również schemat kolorów dla wartości w kolumnie **Ostatnia kopia zapasowa** dla każdego komputera.

Ostatnie połączenie

Ta opcja jest uwzględniana, gdy konsola jest połączona z serwerem zarządzania lub z zarejestrowanym komputerem (s. 380).

Określa ona, czy ma być wyświetlany alert w przypadku, gdy przez pewien czas nie zostanie nawiązane połączenie pomiędzy komputerem zarejestrowanym a serwerem zarządzania, co oznacza, że komputer może nie być centralnie zarządzany (na przykład w przypadku błędu połączenia sieciowego z tym komputerem). Można skonfigurować okres uważany za krytyczny.

Ustawienie wstępne: alert jest wyświetlany, gdy ostatnie połączenie komputera z serwerem zarządzania nastąpiło ponad **5 dni** temu.

Alert jest wyświetlany w sekcji **Alerty** na **Pulpicie nawigacyjnym**. Gdy konsola jest połączona z serwerem zarządzania, to ustawienie określa również schemat kolorów dla wartości w kolumnie **Ostatnie połączenie** dla każdego komputera.

Poświadczenia umożliwiające uzyskanie dostępu do domeny

Ta opcja określa nazwę użytkownika i hasło stosowane przez serwer zarządzania w celu uzyskania dostępu do domeny.

Ustawienie wstępne: Brak poświadczeń

Podczas pracy z grupą dynamiczną opartą na kryterium (s. 337) **Jednostka organizacyjna** serwer zarządzania potrzebuje poświadczeń umożliwiających uzyskanie dostępu do domeny. Jeśli stworzysz taką grupę i omawiana opcja nie zawiera poświadczeń, program wyświetli monit o ich podanie i zapisze je w tej opcji.

Wystarczy określić poświadczenia użytkownika należącego w domenę do grupy **Użytkownicy domeny**.

Powiadomienia pocztą e-mail

Ta opcja umożliwia konfigurowanie powiadomień e-mail.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować powiadamianie pocztą e-mail

1. W polu **Serwer SMTP** wprowadź nazwę serwera SMTP.
2. W polu **Port** ustaw port serwera SMTP. Domyślnie jest to port 25.
3. W polu **Nazwa użytkownika** wprowadź nazwę użytkownika.
4. W polu **Hasło** wprowadź hasło.
5. Kliknij **Dodatkowe parametry poczty e-mail**, aby skonfigurować przedstawione poniżej parametry poczty e-mail, a następnie kliknij **OK**:
 - **Od** — wpisz adres e-mail użytkownika, od którego zostanie wysłana wiadomość. Jeśli pozostawisz to pole puste, wiadomości będą tworzone w taki sposób, jakby pochodziły z adresu docelowego.
 - **Użyj szyfrowania** — umożliwia włączenie szyfrowanego połączenia z serwerem poczty. Można wybrać szyfrowanie SSL lub TLS.
 - Niektórzy dostawcy usług internetowych umożliwiają wysłanie poczty dopiero po uwierzytelnieniu na serwerze poczty przychodzącej. Jeśli tak jest, zaznacz pole wyboru **Zaloguj się na serwerze poczty przychodzącej**, aby umożliwić korzystanie z serwera POP i skonfigurować jego ustawienia:
 - **Serwer poczty przychodzącej (POP)** — wprowadź nazwę serwera POP.
 - **Port** — ustaw port serwera POP. Domyślnie jest to port **110**.
 - **Nazwa użytkownika** — wprowadź nazwę użytkownika.
 - **Hasło** — wprowadź hasło.

6. Kliknij **OK**.

Powiadomienia o alertach

Program Acronis Backup & Recovery 11 umożliwia powiadamianie użytkowników o alertach w formie wiadomości e-mail.

Opcja ta umożliwia określenie godziny i częstotliwości otrzymywania powiadomień o określonych typach alertów.

Ustawienie wstępne: **Wyłączone**.

Uwaga: Przed rozpoczęciem konfigurowania powiadomień o alertach należy określić ustawienia serwera SMTP w sekcji *Powiadomienia pocztą e-mail* (s. 298).

Aby skonfigurować powiadomienia o alertach

1. Zaznacz pole wyboru **Wysyłaj powiadomienia pocztą e-mail**.
2. W polu **Adresy e-mail** wpisz adres e-mail, na który będą wysyłane powiadomienia. Można wprowadzić kilka adresów oddzielonych średnikami.
3. W polu **Temat** wpisz temat wiadomości z powiadomieniem lub pozostaw wartość domyślną.
4. Wybierz wymaganą metodę wysyłania powiadomień:
 - Każdy alert — powiadomienia będą wysyłane natychmiast po odebraniu nowego alertu:
Zaznacz pole wyboru **Natychmiast po wystąpieniu alertu**.
Kliknij **Wybierz typy alertów...**, aby określić typy alertów, o których chcesz otrzymywać powiadomienia.
 - Według harmonogramu — powiadomienie obejmujące wszystkie alerty, jakie wystąpiły w danym okresie. Aby otrzymywać powiadomienia według harmonogramu:
Zaznacz pole wyboru **Według harmonogramu**.
Kliknij **Wybierz typy alertów...**, aby określić typy alertów, o których chcesz otrzymywać powiadomienia.
Kliknij **Harmonogram powiadomień**, aby skonfigurować częstotliwość i godzinę wysyłania powiadomień.
5. Kliknij **OK**.
6. Kliknij **Wyślij próbną wiadomość e-mail**, aby sprawdzić, czy ustawienia są poprawne.

Śledzenie zdarzeń

Serwer zarządzania można skonfigurować tak, aby rejestrował zdarzenia w dzienniku zdarzeń aplikacji systemu Windows, a nie tylko we własnym dzienniku.

Serwer zarządzania można skonfigurować tak, aby wysyłał obiekty SNMP (Simple Network Management Protocol) do określonego menedżera SNMP.

Dziennik zdarzeń systemu Windows

Ta opcja określa, czy serwer zarządzania musi rejestrować zdarzenia własnego dziennika w rejestrze zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, należy uruchomić plik **eventvwr.exe** lub wybrać polecenia **Panel sterowania > Administrative tools (Narzędzia administracyjne) > Event Viewer (Podgląd zdarzeń)**). Zdarzenia do rejestrowania można filtrować.

Wstępnie ustawiona wartość: **Wyłączone**.

Aby włączyć tę opcję, zaznacz pole wyboru **Rejestruj zdarzenia**.

Pole wyboru **Typy rejestrowanych zdarzeń** umożliwia filtrowanie zdarzeń rejestrowanych w dzienniku zdarzeń aplikacji systemu Windows:

- **Wszystkie zdarzenia** — wszystkie zdarzenia (informacje, ostrzeżenia i błędy);
- **Błędy i ostrzeżenia;**
- **Tylko błędy.**

Aby wyłączyć tę opcję, anuluj zaznaczenie pola wyboru **Rejestruj zdarzenia**.

Powiadomienia SNMP

Ta opcja określa, czy serwer zarządzania musi wysyłać zdarzenia własnego dziennika do określonych menedżerów SNMP (Simple Network Management Protocol). Można wybrać typy zdarzeń, które będą wysyłane.

Aby uzyskać szczegółowe informacje na temat programu Acronis Backup & Recovery 11, zobacz „Obsługa SNMP (s. 46)”.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować wysyłanie komunikatów SNMP

1. Zaznacz pole wyboru **Wysyłaj wiadomości do serwera SNMP**.
2. Określ odpowiednie opcje:
 - **Typy wysyłanych zdarzeń** — wybierz typy zdarzeń: **Wszystkie zdarzenia**, **Błędy i ostrzeżenia** lub **Tylko błędy**.
 - **Nazwa/adres IP serwera** — wpisz nazwę lub adres IP hosta, na którym uruchomiona jest aplikacja zarządzająca SNMP, do której chcesz wysyłać komunikaty.
 - **Spółeczność** — wpisz nazwę społeczności SNMP, do której należy host z aplikacją zarządzającą SNMP oraz komputer wysyłający. Typowe ustawienie to „public” („publiczna”).

Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy ustawienia są poprawne.

Aby wyłączyć wysyłanie komunikatów SNMP, wyczyść pole wyboru **Wysyłaj wiadomości do serwera SNMP**.

Komunikaty są wysyłane przy użyciu protokołu UDP.

Poziom dziennika

Ta opcja określa, czy serwer zarządzania ma gromadzić zdarzenia z dzienników na komputerach zarejestrowanych w dzienniku centralnym zapisanym w dedykowanej bazie danych i dostępnym w widoku **Dziennik**. Można ustawić opcję dla wszystkich zdarzeń jednocześnie lub wybrać typy zdarzeń, które mają być gromadzone. W przypadku całkowitego wyłączenia gromadzenia zdarzeń z dzienników w dzienniku centralnym będzie znajdował się wyłącznie dziennik serwera zarządzania.

Ustawienie wstępne: **Zbieraj dzienniki — Wszystkie zdarzenia**.

W celu określenia typów gromadzonych zdarzeń należy użyć pola kombi **Typy rejestrowanych zdarzeń**:

- **Wszystkie zdarzenia** — w dzienniku centralnym rejestrowane są wszystkie zdarzenia (informacje, ostrzeżenia i błędy), które wystąpiły na wszystkich komputerach zarejestrowanych na serwerze zarządzania
- **Błędy i ostrzeżenia** — w dzienniku centralnym rejestrowane są ostrzeżenia i błędy

- **Tylko błędy** — w dzienniku centralnym rejestrowane są tylko błędy

Aby wyłączyć gromadzenie zdarzeń z dzienników, należy anulować zaznaczenie pola wyboru **Zbieraj dzienniki**.

Reguły czyszczenia dziennika

Ta opcja określa sposób czyszczenia centralnego dziennika zdarzeń przechowywanego w bazie danych raportowania serwera zarządzania.

Opcja definiuje maksymalny rozmiar bazy danych raportowania.

Ustawienie wstępne: **Maksymalny rozmiar dziennika: 1 GB. Podczas czyszczenia zachowaj 95% maksymalnego rozmiaru dziennika.**

Po włączeniu tej opcji program będzie co 100 wpisów dziennika porównywał jego bieżący rozmiar z rozmiarem maksymalnym. Gdy maksymalny rozmiar dziennika zostanie przekroczony, program usunie najstarsze wpisy. Można wybrać liczbę zachowywanych wpisów dziennika. Ustawienie domyślne 95% oznacza zachowanie większości dziennika. Ustawienie minimalne 1% oznacza praktycznie wyczyszczenie dziennika.

Nawet przy usuniętych limicie rozmiaru dziennika rejestrowanie zdarzeń w bazie danych SQL Server Express zostanie przerwane, gdy dziennik osiągnie rozmiar 4 GB. Wynika to z obowiązującego w programie SQL Express Edition limitu rozmiaru bazy danych wynoszącego 4 GB. Jeśli chcesz maksymalnie wykorzystać pojemność bazy danych SQL Express, ustaw maksymalny rozmiar dziennika na około 3,8 GB.

Parametr ten można także ustawić za pomocą szablonu Acronis Administrative Template (s. 365).

Serwer proxy kopii zapasowej online

Ta opcja jest dostępna tylko w przypadku połączenia z magazynem Acronis Online Backup Storage za pośrednictwem Internetu.

Ta opcja określa, czy serwer zarządzania ma łączyć się z Internetem za pośrednictwem serwera proxy.

Uwaga: Funkcja Acronis Backup & Recovery Online obsługuje wyłącznie serwery proxy HTTP i HTTPS.

Ustawienia proxy agenta i serwera zarządzania są konfigurowane oddzielnie, nawet jeśli agent i serwer są zainstalowane na tym samym komputerze.

Aby skonfigurować ustawienia serwera proxy

1. Zaznacz pole wyboru **Użyj serwera proxy**.
2. W polu **Adres** określ nazwę sieciową lub adres IP serwera proxy — na przykład: **proxy.example.com** lub **192.168.0.1**
3. W polu **Port** określ numer portu serwera proxy — na przykład: **80**
4. Jeśli serwer proxy wymaga uwierzytelniania, określ poświadczenia w polach **Nazwa użytkownika** i **Hasło**.
5. Aby sprawdzić poprawność ustawień serwera proxy, kliknij **Sprawdź połączenie**.

11.4 Konfigurowanie komponentów programu Acronis Backup & Recovery 11

W systemie Windows różne parametry komponentów programu Acronis Backup & Recovery 11 można skonfigurować na trzy sposoby:

- przy użyciu szablonu administracyjnego Acronis Administrative Template;
- przy użyciu graficznego interfejsu użytkownika,
- przez modyfikację rejestru systemu Windows.

W systemie Linux szablon administracyjny i rejestr nie są używane. Parametry konfiguruje się przez edycję odpowiednich plików konfiguracyjnych.

Jeśli wartości dowolnego z tych parametrów skonfigurowane przy użyciu szablonu administracyjnego różnią się od wartości skonfigurowanych w graficznym interfejsie użytkownika, wartości z szablonu mają pierwszeństwo i są uwzględniane od razu, a parametry przedstawione w graficznym interfejsie użytkownika są odpowiednio zmieniane.

W poniższych podtematach opisano poszczególne sposoby konfiguracji oraz parametry, które można za ich pomocą ustawić.

11.4.1 Parametry konfigurowane przy użyciu szablonu administracyjnego

Poniżej podano parametry komponentów Acronis Backup & Recovery 11, które można skonfigurować przy użyciu szablonu administracyjnego Acronis Administrative Template. Aby uzyskać informacje na temat sposobu stosowania szablonu administracyjnego, zobacz „Jak załadować szablon Acronis Administrative Template” (s. 360).

Szablon administracyjny zawiera parametry konfiguracyjne agenta Acronis Backup & Recovery 11 Agent, serwera zarządzania Acronis Backup & Recovery 11 Management Server i węzła magazynowania Acronis Backup & Recovery 11 Storage Node oraz wspólne parametry komponentów Acronis Backup & Recovery 11.

Parametry węzła magazynowania Acronis Backup & Recovery 11 Storage Node zostały opisane w sekcji „Węzły magazynowania” (s. 219). Pozostałe parametry zostały opisane w odpowiednich podtematach.

Jak załadować szablon Acronis Administrative Template

Szablon administracyjny Acronis Administrative Template umożliwia precyzyjne konfigurowanie niektórych funkcji związanych z zabezpieczeniami, w tym ustawień zaszyfrowanej komunikacji. Korzystając z mechanizmu zasad grupy firmy Microsoft, ustawienia zasad szablonu można zastosować do pojedynczego komputera, jak również do całej domeny.

Aby załadować szablon Acronis Administrative Template

1. Uruchom Edytor obiektów zasad grupy w systemie Windows (%windir%\system32\gpedit.msc).
2. Otwórz obiekt zasad grupy (GPO), który chcesz edytować.
3. Rozwiń węzeł **Konfiguracja komputera**.
4. Kliknij prawym przyciskiem myszy **Szablony administracyjne**.
5. Kliknij **Dodaj/Usuń szablony**.
6. Kliknij **Dodaj**.

7. Przejdź do szablonu Acronis Administrative Template (\Program Files\Common Files\Acronis\Agent \Acronis_agent.adm lub \Program Files\Acronis\BackupAndRecoveryConsole\Acronis_agent.adm) i kliknij **Otwórz**.

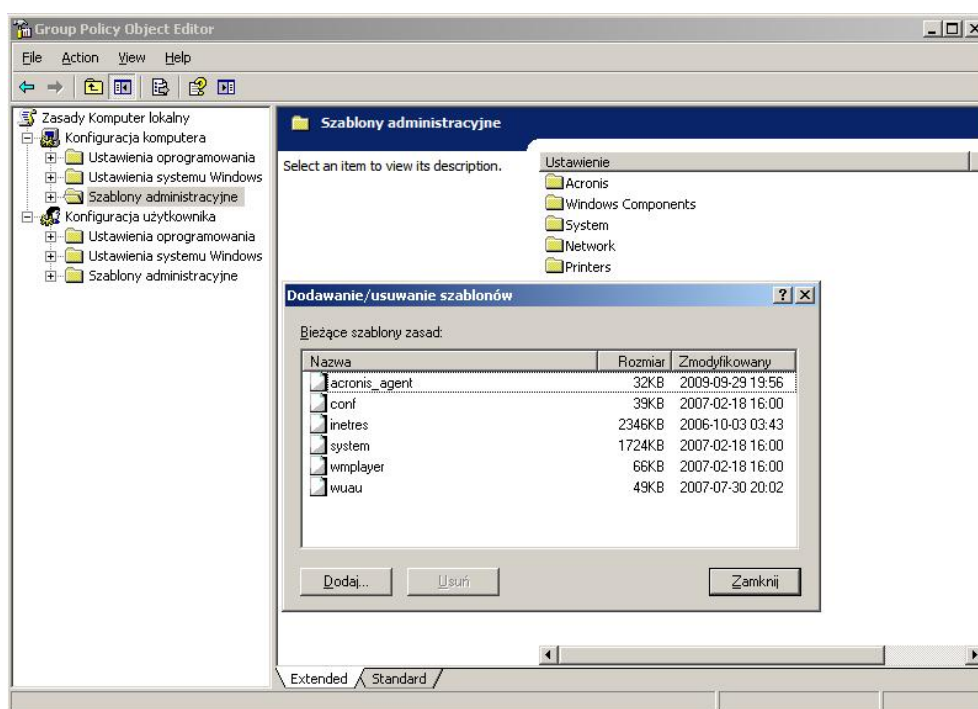
Łaadowany szablon można otworzyć i zmodyfikować żądane ustawienia. Po ładowaniu szablonu lub zmodyfikowaniu jego ustawień należy ponownie uruchomić skonfigurowane komponenty lub niektóre z ich usług.

Szczegółowe informacje na temat edytora obiektów zasad grupy w systemie Windows są dostępne pod adresem:

<http://msdn2.microsoft.com/pl-pl/library/aa374163.aspx>

Szczegółowe informacje na temat zasad grup są dostępne pod adresem:

<http://msdn2.microsoft.com/pl-pl/library/aa374177.aspx>



Acronis Backup & Recovery 11 Agent dla systemu Windows

Poniżej znajdują się parametry agenta Acronis Backup & Recovery 11, które można ustawić za pomocą szablonu Acronis Administrative Template.

Licencjonowanie

Określa, jak często agent kontroluje licencję na serwerze licencji i ile czasu może pracować bez serwera licencji.

License Check Interval (w dniach)

Opis: Określa (w dniach) częstotliwość sprawdzania dostępności licencji na serwerze Acronis License Server.

Możliwe wartości: Dowlolna liczba całkowita z zakresu od **0** do **5**

Wartość domyślna: **1**

Agent Acronis Backup & Recovery 11 kontroluje regularnie, czy na serwerze licencji znajduje się klucz licencji. Pierwsze sprawdzenie odbywa się przy każdym uruchomieniu agenta

programu Acronis Backup & Recovery 11, a następnie obecność licencji sprawdzana jest z częstotliwością określoną w dniach w ustawieniu **License Check Interval**.

Gdy agent nie może się połączyć z serwerem licencji, w dzienniku agenta umieszczane jest ostrzeżenie. Można je wyświetlić na pulpicie nawigacyjnym..

Jeśli ustawienie ma wartość **0**, obecność licencji nie będzie sprawdzana. Brak licencji spowoduje, że program Acronis Backup & Recovery 11 przestanie działać po upływie liczby dni określonej w ustawieniu **Maximum Time Without License Server** (zobacz następny parametr).

Zobacz także ustawienie **License Server Connection Retry Interval** w dalszej części tego tematu.

Maximum Time Without License Server (w dniach)

Opis: Określa czas (w dniach), po upływie którego program Acronis Backup & Recovery 11 przestanie działać.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **60**

Wartość domyślna: **30**

Jeśli serwer licencji Acronis License Server będzie niedostępny, program Acronis Backup & Recovery 11 będzie działać w pełni funkcjonalnie przez liczbę dni określoną w ustawieniu **Maximum Time Without License Server**. Czas ten jest liczony od chwili instalacji lub ostatniego pomyślnego sprawdzenia licencji.

License Server Connection Retry Interval (w godzinach)

Opis: Określa odstęp (w godzinach) między próbami połączenia, gdy serwer licencji Acronis License Server jest niedostępny.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **24**

Wartość domyślna: **1**

Jeśli podczas sprawdzania dostępności klucza licencyjnego (zobacz ustawienie **License Check Interval** we wcześniejszej części tego tematu) agent programu Acronis Backup & Recovery 11 nie będzie mógł połączyć się z serwerem licencji, ponowi próbę połączenia po upływie liczby godzin określonej w ustawieniu **License Server Connection Retry Interval**.

Jeśli ustawienie ma wartość **0**, próby ponownego połączenia nie będą podejmowane. Agent sprawdzi dostępność licencji po upływie czasu, który określono w ustawieniu **License Check Interval**.

License Server Address

Opis: Określa nazwę sieciową lub adres IP serwera Acronis License Server.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Log Cleanup Rules

Określa sposób czyszczenia dziennika agenta.

Ten parametr ma następujące ustawienia:

Max Size

Opis: Określa maksymalny (w kilobajtach) rozmiar folderu z dziennikiem agenta.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **1048576** (1 GB)

Percentage To Keep

Opis: Określa procentowo maksymalny rozmiar dziennika, który ma być zachowany podczas czyszczenia.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **95**

Aby zapoznać się ze szczegółami dotyczącymi czyszczenia dziennika agenta, zobacz Reguły czyszczenia dziennika (s. 302).

Windows Event Log

Określa, kiedy zdarzenia agenta Acronis Backup & Recovery 11 mają być zapisywane w dzienniku zdarzeń Aplikacji systemu Windows.

Parametr ten przyjmuje dwa ustawienia:

Trace State

Opis: Określa, czy zdarzenia dotyczące agenta mają być rejestrowane w dzienniku zdarzeń.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

Trace Level

Opis: Określa minimalny poziom ważności zdarzeń rejestrowanych w dzienniku zdarzeń. Rejestrowane będą wyłącznie zdarzenia o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), lub **5** (błąd krytyczny)

Wartość domyślna: **4** (będą wysyłane tylko błędy i błędy krytyczne — jeśli ustawienie **Trace State** ma wartość **True**)

SNMP

Określa typy zdarzeń agenta, które będą wysyłały powiadomienia za pomocą protokołu SNMP.

Ten parametr ma następujące ustawienia:

Trace State

Opis: Określa, czy mają być wysyłane powiadomienia SNMP.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

Trace Level

Opis: Określa minimalny poziom ważności zdarzeń, o których mają być wysyłane powiadomienia SNMP. Wysyłane będą wyłącznie powiadomienia dotyczące zdarzeń o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), lub **5** (błąd krytyczny)

Wartość domyślna: **4** (będą wysyłane tylko błędy i błędy krytyczne — jeśli ustawienie **Trace State** ma wartość **True**)

SNMP Address

Opis: Określa nazwę sieciową lub adres IP serwera SNMP.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

SNMP Community

Opis: Określa nazwę społeczności do powiadomień SNMP.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: **public**

Backup

Określa lokalizację i początkowy rozmiar magazynu migawki — pliku tymczasowego używanego podczas tworzenia kopii zapasowej danych za pomocą migawki. Plik ten jest usuwany zaraz po zakończeniu tworzenia kopii zapasowej.

Przy domyślnych ustawieniach magazyn migawki jest tworzony w folderze plików tymczasowych agenta i początkowo zajmuje 20 procent miejsca dostępnego na woluminie zawierającym dany folder. Rozmiar ten może wzrosnąć, jeśli migawka wymaga więcej miejsca.

Warto rozważyć zwiększenie początkowego rozmiaru magazynu migawki lub umieszczenie go na innym woluminie, jeśli występują problemy podczas tworzenia kopii zapasowej danych, które często ulegają zmianie podczas tworzenia kopii.

Parametr używany podczas tworzenia lokalnego planu tworzenia kopii zapasowych. Zmiana tego parametru nie wpływa na istniejące lokalne plany tworzenia kopii zapasowych.

Ten parametr ma następujące ustawienia:

Snapshot Storage Path

Opis: Określa folder, w którym zostanie utworzony magazyn migawki.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Pusty ciąg oznacza folder %AllUsersProfile%\Application Data\Acronis\BackupAndRecovery\MMS\Temp.

Można określić lokalny folder na dowolnym woluminie, także tym, dla którego jest wykonywana kopia zapasowa.

Snapshot Storage Absolute Size

Opis: Określa w megabajtach początkowy rozmiar magazynu migawki.

Możliwe wartości: Dowolna liczba całkowita z zakresu od 0 do **2147483647**

Wartość domyślna: 0

Wartość 0 oznacza, że serwer zarządzania użyje ustawienia **Snapshot Storage Relative Size**.

Rozmiar początkowy nie może być większy niż ilość dostępnego miejsca minus 50 MB.

Snapshot Storage Relative Size

Ustawienie to jest efektywne tylko wtedy, gdy ustawienie **Snapshot Storage Absolute Size** wynosi 0.

Opis: Określa początkowy rozmiar magazynu migawki jako procent miejsca dostępnego na dysku podczas uruchamiania procesu tworzenia kopii zapasowej.

Możliwe wartości: Dowolna liczba całkowita z zakresu od 0 do 100

Wartość domyślna: 20

Wartość 0 oznacza, że magazyn migawki nie zostanie utworzony.

Rozmiar początkowy nie może być większy niż ilość dostępnego miejsca minus 50 MB.

Migawki można wykonywać nawet bez magazynu.

Rozmiar magazynu migawki nie wpływa na rozmiar kopii zapasowej.

Online Backup

Określa ustawienia serwera proxy w przypadku połączenia z magazynem Acronis Online Backup Storage za pośrednictwem Internetu.

Ten parametr ma następujące ustawienia:

Proxy Server Enabled

Opis: Określa, czy ma być używany serwer proxy.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

Jeśli wartością tego parametru jest **False**, wszystkie następujące parametry są ignorowane.

Proxy Server Name

Opis: Określa nazwę sieciową lub adres IP serwera proxy

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Proxy Server Port

Opis: Określa numer portu serwera proxy

Możliwe wartości: Dowolna liczba całkowita z zakresu od 0 do 65535

Wartość domyślna: **0**

Jeśli serwer proxy wymaga uwierzytelniania, użyj następujących dwóch parametrów.

Proxy Server User Name

Opis: Określa nazwę użytkownika uwierzytelnianego na serwerze proxy

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Proxy Server User Password

Opis: Określa hasło uwierzytelniania na serwerze proxy

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Ważne. Hasło jest widoczne dla każdego użytkownika dysponującego dostępem do szablonu administracyjnego, na przykład administratora komputera.

Acronis Backup & Recovery 11 Management Server

Poniżej znajdują się parametry serwera Acronis Backup & Recovery 11, które można ustawić za pomocą szablonu Acronis Administrative Template.

Collecting Logs

Określa, kiedy jest wykonywane zbieranie dzienników z komputerów zarządzanych przez serwer Acronis Backup & Recovery 11 Management Server.

Parametr ten przyjmuje dwa ustawienia:

Trace State

Opis: Określa, czy z komputerów zarejestrowanych mają być zbierane wpisy dzienników na temat zdarzeń dotyczących komponentów.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **True**

Trace Level

Opis: Określa minimalny poziom ważności zbieranych wpisów. Zbierane będą wyłącznie wpisy o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), lub **5** (błąd krytyczny)

Wartość domyślna: **0** (zbierane będą wszystkie wpisy)

Log Cleanup Rules

Określa sposób czyszczenia centralnego dziennika zdarzeń przechowywanego w bazie danych raportowania serwera zarządzania.

Ten parametr ma następujące ustawienia:

Max Size

Opis: Określa maksymalny (w kilobajtach) rozmiar centralnego dziennika zdarzeń.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **1048576** (1 GB)

Percentage to Keep

Opis: Określa procentowo maksymalny rozmiar dziennika, który ma być zachowany podczas czyszczenia.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **95**

Aby zapoznać się ze szczegółami dotyczącymi czyszczenia centralnego dziennika zdarzeń, zobacz Reguły czyszczenia dziennika (s. 359).

Windows Event Log

Określa, kiedy zdarzenia serwera zarządzania Acronis Backup & Recovery 11 mają być zapisywane w dzienniku zdarzeń Aplikacje systemu Windows.

Parametr ten przyjmuje dwa ustawienia:

Trace State

Opis: Określa, czy zdarzenia dotyczące serwera Acronis Backup & Recovery 11 Management Server mają być rejestrowane w dzienniku zdarzeń.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

Trace Level

Opis: Określa minimalny poziom ważności zdarzeń rejestrowanych w dzienniku zdarzeń. Rejestrowane będą wyłącznie zdarzenia o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), lub **5** (błąd krytyczny)

Wartość domyślna: **4** (będą wysyłane tylko błędy i błędy krytyczne — jeśli ustawienie **Trace State** ma wartość **True**)

SNMP

Określa typy zdarzeń serwera zarządzania, które będą wysyłały powiadomienia za pomocą protokołu SNMP.

Ten parametr ma następujące ustawienia:

Trace State

Opis: Określa, czy mają być wysyłane powiadomienia SNMP.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

Trace Level

Opis: Określa minimalny poziom ważności zdarzeń, o których mają być wysyłane powiadomienia SNMP. Wysyłane będą wyłącznie powiadomienia dotyczące zdarzeń o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), lub **5** (błąd krytyczny)

Wartość domyślna: **4** (będą wysyłane tylko błędy i błędy krytyczne — jeśli ustawienie **Trace State** ma wartość **True**)

SNMP Address

Opis: Określa nazwę sieciową lub adres IP serwera SNMP.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

SNMP Community

Opis: Określa nazwę społeczności do powiadomień SNMP.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: **public**

Synchronizacja

Określa sposób łączenia się serwera Acronis Backup & Recovery 11 Management Server z komputerami zarejestrowanymi w celu wdrażania scentralizowanych planów tworzenia kopii zapasowych, pobierania dzienników i informacji o stanie planów tworzenia kopii zapasowych oraz wykonywania podobnych czynności — ogólnie nazywanych synchronizacją.

Ten parametr ma następujące ustawienia:

Maximum Connections

Opis: Określa maksymalną liczbę równoczesnych aktywnych połączeń synchronizacji.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **1** do **500**

Wartość domyślna: **200**

Jeśli łączna liczba komputerów zarejestrowanych online nie przekracza wartości **Maximum Connections**, połączenia z tymi komputerami są zawsze aktywne, a serwer zarządzania regularnie przeprowadza synchronizację z każdym komputerem.

W przeciwnym przypadku liczba zarejestrowanych komputerów zależy od przydzielonej liczby jednoczesnych połączeń. Po wykonaniu synchronizacji komputera, serwer zarządzania może odłączyć się od niego i wykorzystać nieużywane połączenie do synchronizacji innego komputera itd.

(Uwaga: Połączenia z komputerami o wysokim priorytecie synchronizacji — zobacz **Period-High Priority** w dalszej części tego tematu — zazwyczaj są stale aktywne).

Połączenia synchronizacyjne są niezależne od połączeń między programami, np. między serwerem Acronis Backup & Recovery 11 Management Server i konsolą Acronis Backup & Recovery 11 Management Console.

Maximum Workers

Opis: Określa maksymalną liczbę wątków synchronizacji.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **1** do **100**

Wartość domyślna: **30**

W celu synchronizacji zarejestrowanego komputera, z którym zostało już nawiązane połączenie, serwer zarządzania wykorzystuje specjalne wątki nazywane wątkami roboczymi.

Każdy wątek roboczy wykonuje w danym momencie synchronizację dokładnie jednego komputera.

Podłączony komputer do synchronizacji oczekuje na dostępność wątku roboczego. Z tego względu rzeczywista liczba wątków roboczych nigdy nie przekracza maksymalnej liczby połączeń (zobacz ustawienie **Maximum Connections** opisane powyżej).

Period (w sekundach)

Opis: Określa (w sekundach) częstotliwość wykonywania synchronizacji na komputerach o normalnym priorytecie synchronizacji — zwykle są to komputery, na których aktualnie nie są uruchomione scentralizowane zadania tworzenia kopii zapasowych.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **120** do **2147483647**

Wartość domyślna: **120**

Serwer Acronis Backup & Recovery 11 Management Server próbuje wykonać jedną synchronizację każdego komputera o normalnym priorytecie w czasie określonym (w sekundach) w ustawieniu **Period**, korzystając w tym celu z dostępnego wątku roboczego (zobacz ustawienie **Maximum Workers** opisane powyżej).

Jeśli liczba wątków roboczych jest niższa od komputerów o standardowym priorytecie, rzeczywisty odstęp między synchronizacjami może być dłuższy od wartości danego parametru.

Period-High Priority (sekund)

Opis: Określa (w sekundach) częstotliwość wykonywania synchronizacji na komputerach o wysokim priorytecie synchronizacji — zwykle są to komputery, na których aktualnie są uruchomione scentralizowane zadania tworzenia kopii zapasowych.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **15** do **2147483647**

Wartość domyślna: **15**

Jest to parametr analogiczny do parametru **Period** opisanego powyżej.

Real-Time Monitoring

Opis: Określa, czy komputery zarejestrowane należy monitorować w czasie rzeczywistym, zamiast stosować mechanizm sondowania.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

W domyślnej konfiguracji serwer Acronis Backup & Recovery 11 łączy się z zarejestrowanymi komputerami w celu wykonania synchronizacji danych; w szczególności, w celu pobrania np. dzienników kopii zapasowych. Jest to znane jako mechanizm odpytywania.

Jeśli ustawienie **Real Time Monitoring** ma wartość **True**, zawsze po pojawieniu się nowych danych serwer zarządzania wysyła do komputerów żądanie udostępnienia tych danych, a następnie przechodzi do trybu nasłuchiwania. Jest to znane jako bieżący monitoring.

Pozwala on na zmniejszenie ilości danych przesyłanych przez sieć, np. gdy scentralizowane zadania tworzenia kopii zapasowych są wykonywane rzadko. Jednak ustawienie to działa skutecznie tylko wtedy, gdy liczba zarejestrowanych komputerów jest ograniczona.

Monitorowania w czasie rzeczywistym nie należy włączać, gdy liczba komputerów zarejestrowanych przekracza maksymalną liczbę równoczesnych połączeń (zobacz **Maximum Connections** we wcześniejszej części tego tematu).

Second Connection Attempt

Opis: Określa, czy należy wykonać próbę połączenia się z komputerem zarejestrowanym przy użyciu jego ostatniego znanego adresu IP, jeśli próba połączenia z tym komputerem przy użyciu nazwy hosta zakończyła się niepowodzeniem.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

Podczas próby połączenia z zarejestrowanym komputerem, serwer Acronis Backup & Recovery 11 Management Server próbuje najpierw użyć nazwy sieciowej komputera, jeśli została wprowadzona.

Jeśli ustawienie **Second Connection Attempt** ma wartość **True** i połączenie z komputerem przy użyciu jego nazwy sieciowej zakończyło się niepowodzeniem, serwer zarządzania spróbuje połączyć się z tym komputerem przy użyciu ostatniego adresu IP skojarzonego z jego nazwą sieciową.

Określenie wartości **True** w ustawieniu Second Connection Attempt jest zalecane tylko w sieciach, w których często występują problemy z serwerami DNS, a adresy IP komputerów zmieniają się rzadko, tak jak w przypadku stałych adresów IP lub długich czasów dzierżawy DHCP.

Ustawienie to nie odnosi się do komputerów, które zostały dodane do serwera zarządzania za pomocą adresu IP.

Próg w trakcie trybu offline (w sekundach)

Opis: Określa maksymalny odstęp (w sekundach) między kolejnymi próbami połączenia się z komputerem zarejestrowanym, który wydaje się znajdować w trybie offline.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **120** do **2147483647**

Wartość domyślna: **1800**

Zwykle serwer zarządzania łączy się z każdym komputerem zarejestrowanym co pewien czas (zobacz ustawienia **Period** i **Period-High Priority** we wcześniejszych częściach tej sekcji). Jeśli serwer zarządzania wykryje, że komputer jest w trybie offline, czas ten zostanie podwojony i będzie podwajany przy każdej kolejnej próbie aż do osiągnięcia wartości określonej w ustawieniu **Offline Period Threshold**. Gdy komputer wróci do trybu online, odstęp czasu zostanie przywrócony do normalnego.

Pozwala to zwiększyć wydajność wykorzystania zasobów serwera zarządzania i zmniejszyć obciążenie sieci.

Backup

Określa lokalizację i początkowy rozmiar magazynu migawki — pliku tymczasowego używanego podczas tworzenia kopii zapasowej danych za pomocą migawki. Plik ten jest usuwany zaraz po zakończeniu tworzenia kopii zapasowej.

Przy domyślnych ustawieniach magazyn migawki jest tworzony w folderze plików tymczasowych odpowiedniego agenta i początkowo zajmuje 20 procent miejsca dostępnego na woluminie zawierającym dany folder. Rozmiar ten może wzrosnąć, jeśli migawka wymaga więcej miejsca.

Warto rozważyć zwiększenie początkowego rozmiaru magazynu migawki lub umieszczenie go na innym woluminie, jeśli występują problemy podczas tworzenia kopii zapasowej danych, które często ulegają zmianie podczas tworzenia kopii.

Parametr używany podczas tworzenia scentralizowanego planu tworzenia kopii zapasowych. Zmiana tego parametru nie wpływa na istniejące scentralizowane plany tworzenia kopii zapasowych.

Ten parametr ma następujące ustawienia:

Snapshot Storage Path

Opis: Określa folder, w którym zostanie umieszczony magazyn migawki.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Pusty ciąg oznacza folder %AllUsersProfile%\Application Data\Acronis\BackupAndRecovery\MMS\Temp.

Można określić lokalny folder na dowolnym woluminie, także tym, dla którego jest wykonywana kopia zapasowa.

Snapshot Storage Absolute Size

Opis: Określa w megabajtach początkowy rozmiar magazynu migawki.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **0**

Wartość **0** oznacza, że serwer zarządzania użyje ustawienia **Snapshot Storage Relative Size**.

Rozmiar początkowy nie może być większy niż ilość dostępnego miejsca minus 50 MB.

Snapshot Storage Relative Size

Ustawienie to jest efektywne tylko wtedy, gdy ustawienie **Snapshot Storage Absolute Size** wynosi **0**.

Opis: Określa początkowy rozmiar magazynu migawki jako procent miejsca dostępnego na dysku podczas uruchamiania procesu tworzenia kopii zapasowej.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **20**

Wartość **0** oznacza, że magazyn migawki nie zostanie utworzony.

Rozmiar początkowy nie może być większy niż ilość dostępnego miejsca minus 50 MB.

Migawki można wykonywać nawet bez magazynu.

Rozmiar magazynu migawki nie wpływa na rozmiar kopii zapasowej.

Online Backup

Określa ustawienia serwera proxy w przypadku połączenia z magazynem Acronis Online Backup Storage za pośrednictwem Internetu.

Ten parametr ma następujące ustawienia:

Proxy Server Enabled

Opis: Określa, czy ma być używany serwer proxy.

Możliwe wartości: **True** lub **False**

Wartość domyślna: **False**

Jeśli wartością tego parametru jest **False**, wszystkie następujące parametry są ignorowane.

Proxy Server Name

Opis: Określa nazwę sieciową lub adres IP serwera proxy

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Proxy Server Port

Opis: Określa numer portu serwera proxy

Możliwe wartości: Dowolna liczba całkowita z zakresu od 0 do 65535

Wartość domyślna: **0**

Jeśli serwer proxy wymaga uwierzytelniania, użyj następujących dwóch parametrów.

Proxy Server User Name

Opis: Określa nazwę użytkownika uwierzytelnianego na serwerze proxy

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Proxy Server User Password

Opis: Określa hasło uwierzytelniania na serwerze proxy

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Ważne. Hasło jest widoczne dla każdego użytkownika dysponującego dostępem do szablonu administracyjnego, na przykład administratora komputera.

Acronis Backup & Recovery 11

W tej sekcji przy użyciu szablonu administracyjnego określono parametry połączenia oraz parametry śledzenia zdarzeń dotyczących następujących komponentów programu Acronis Backup & Recovery 11:

- Acronis Backup & Recovery 11 Management Server
- Acronis Backup & Recovery 11 Agent
- Acronis Backup & Recovery 11 Storage Node

Parametry połączenia

Porty zdalnego agenta

Określa port, którego komponent będzie używać do komunikacji przychodzącej i wychodzącej z innymi komponentami Acronis.

Wybierz jedną z następujących opcji:

Nieskonfigurowane

Komponent będzie używać domyślnego numeru portu TCP 9876.

Włączone

Komponent będzie używać określonego portu. Wpisz numer portu w polu **Port TCP serwera**.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Opcje szyfrowania klienta

Określa, czy przesyłane dane mają być szyfrowane, gdy komponent służy jako aplikacja kliencka, a także czy należy ufać certyfikatom SSL z podpisem własnym.

Wybierz jedną z następujących opcji:

Nieskonfigurowane

Komponent będzie używać ustawień domyślnych, czyli będzie w miarę możliwości korzystać z szyfrowania oraz ufać certyfikatom SSL z podpisem własnym (zobacz poniższą opcję).

Włączone

Szyfrowanie jest włączone. Wybierz jedno z następujących ustawień opcji **Szyfrowanie**:

Włączone

Przesyłane dane będą szyfrowane, jeśli szyfrowanie zostało włączone w aplikacji serwerowej. W przeciwnym razie dane nie będą szyfrowane.

Wyłączone

Szyfrowanie jest wyłączone. Nie będzie można nawiązać żadnego połączenia z aplikacją serwerową, która wymaga szyfrowania.

Wymagane

Dane będą przesyłane tylko w przypadku, gdy szyfrowanie zostało włączone w aplikacji serwerowej (zobacz sekcję „Opcje szyfrowania serwera”). Przesyłane dane będą szyfrowane.

Parametry uwierzytelniania

Zaznaczenie pola wyboru **Ufaj certyfikatom z podpisem własnym** umożliwia klientowi łączenie się z aplikacjami serwerowymi, które używają certyfikatów SSL z podpisem własnym, takich jak certyfikaty utworzone podczas instalacji komponentów programu Acronis Backup & Recovery 11 (zobacz Certyfikaty SSL (s. 313)).

To pole wyboru powinno być zaznaczone, chyba że w danym środowisku używana jest infrastruktura klucza publicznego (PKI).

Wybierz jedno z następujących ustawień opcji **Użyj uwierzytelniania certyfikatu agenta**:

Nie używaj

Użycie certyfikatów SSL jest wyłączone. Nie będzie można nawiązać żadnych połączeń z aplikacją serwerową, która wymaga użycia certyfikatów SSL.

Użyj, jeśli to możliwe

Użycie certyfikatów SSL jest włączone. Klient będzie używać certyfikatów SSL, jeśli zostały one włączone w aplikacji serwerowej. W przeciwnym razie certyfikaty SSL nie będą używane.

Zawsze używaj

Użycie certyfikatów SSL jest włączone. Połączenie zostanie nawiązane tylko w przypadku, gdy użycie certyfikatów SSL zostało włączone w aplikacji serwerowej.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Opcje szyfrowania serwera

Określa, czy przesyłane dane mają być szyfrowane, gdy komponent służy jako aplikacja serwerowa.

Wybierz jedną z następujących opcji:

Nieskonfigurowane

Komponent będzie używać ustawienia domyślnego, czyli będzie w miarę możliwości korzystać z szyfrowania (zobacz poniższą opcję).

Włączone

Szyfrowanie jest włączone. Wybierz jedno z następujących ustawień opcji **Szyfrowanie**:

Włączone

Przesyłane dane będą szyfrowane, jeśli szyfrowanie zostało włączone w aplikacji klienckiej. W przeciwnym razie dane nie będą szyfrowane.

Wyłączone

Szyfrowanie jest wyłączone. Nie będzie można nawiązać żadnego połączenia z aplikacją kliencką, która wymaga szyfrowania.

Wymagane

Dane będą przesyłane tylko w przypadku, gdy szyfrowanie zostało włączone w aplikacji klienckiej (zobacz sekcję „Opcje szyfrowania klienta”). Przesyłane dane będą szyfrowane.

Parametry uwierzytelniania

Wybierz jedno z następujących ustawień opcji **Użyj uwierzytelniania certyfikatu agenta**:

Nie używaj

Użycie certyfikatów SSL jest wyłączone. Nie będzie można nawiązać żadnych połączeń z aplikacją kliencką, która wymaga użycia certyfikatów SSL.

Użyj, jeśli to możliwe

Użycie certyfikatów SSL jest włączone. Serwer będzie używać certyfikatów SSL, jeśli zostały one włączone w aplikacji klienckiej. W przeciwnym razie certyfikaty SSL nie będą używane.

Zawsze używaj

Użycie certyfikatów SSL jest włączone. Połączenie zostanie nawiązane tylko w przypadku, gdy użycie certyfikatów SSL zostało włączone w aplikacji klienckiej.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Parametry śledzenia zdarzeń

W systemie Windows zdarzenia występujące w programie Acronis Backup & Recovery 11 można rejestrować w dzienniku zdarzeń, pliku lub w obu miejscach.

Każde zdarzenie ma poziom ważności od zera do pięciu, jak to przedstawiono w następującej tabeli:

Poziom	Nazwa	Opis
0	Nieznany	Zdarzenie, którego poziom ważności jest nieznany lub go nie dotyczy
1	Debugowanie	Zdarzenie służące do celów debugowania
2	Informacja	Zdarzenie informacyjne, takie jak informacja o pomyślnym ukończeniu operacji lub uruchomieniu usługi
3	Ostrzeżenie	Zdarzenie wskazujące na możliwy i nieuchronnie zbliżający się problem, taki jak mało wolnego miejsca w skarbcu
4	Błąd	Zdarzenie występujące w efekcie utraty danych lub zatrzymania działania
5	Krytyczny	Zdarzenie występujące w efekcie zakończenia procesu, takiego jak proces agenta

Parametry śledzenia zdarzeń są określone przez następujące ustawienia w szablonie administracyjnym:

File Trace Minimal Level (Minimalny poziom śledzenia plików)

Opis: Określa minimalny poziom ważności zdarzeń rejestrowanych w pliku. Będą rejestrowane wyłącznie zdarzenia o poziomie ważności równym wartości ustawienia **File Trace Minimal Level** (Minimalny poziom śledzenia plików) lub od niej wyższym.

Możliwe wartości: Dowolny poziom ważności od **nieznanego** do **krytycznego** lub **zablokowany**, aby nie rejestrować żadnych zdarzeń.

Wartość domyślna: 2 (oznacza, że będą rejestrowane zdarzenia o poziomach ważności od 2 do 5)

Pliki dzienników znajdują się w folderze **%ALLUSERSPROFILE%\Application Data\Acronis**, w podfolderze **Logs** konkretnego komponentu.

Win32 Trace Minimal Level (Minimalny poziom śledzenia Win32)

Opis: Określa minimalny poziom ważności zdarzeń rejestrowanych w dzienniku zdarzeń systemowych. Będą rejestrowane wyłącznie zdarzenia o poziomie ważności równym wartości ustawienia **Win32 Trace Minimal Level** (Minimalny poziom śledzenia Win32) lub od niej wyższym.

Możliwe wartości: Dowolny poziom ważności od **nieznanego** do **krytycznego** lub **zablokowany**, aby nie rejestrować żadnych zdarzeń.

Wartość domyślna: 4 (oznacza, że będą rejestrowane zdarzenia dotyczące błędów i błędów krytycznych)

Program jakości obsługi klienta

Określa, czy komputer, na którym jest zainstalowany komponent Acronis Backup & Recovery 11, zostanie objęty Programem jakości obsługi klienta.

Wybierz jedną z następujących opcji:

Nieskonfigurowane

Domyślnie komputer nie jest objęty Programem jakości obsługi klienta.

Włączone

W sekcji **Włącz wysyłanie raportów do firmy Acronis** wybierz jedną z następujących opcji:

Włącz

Informacje na temat konfiguracji sprzętowej, najczęściej i najrzadziej używanych funkcji oraz wszelkich problemów będą automatycznie zbierane z komputera i regularnie wysyłane do firmy Acronis. Wyniki końcowe posłużą do udoskonalenia i zwiększenia funkcjonalności oprogramowania w celu lepszego dostosowania go do potrzeb klientów firmy Acronis. Firma Acronis nie zbiera żadnych danych osobowych. Warunki uczestnictwa można znaleźć w witrynie internetowej firmy Acronis.

Wyłącz

Informacje nie będą wysyłane.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

11.4.2 Parametry konfigurowane w graficznym interfejsie użytkownika

W graficznym interfejsie użytkownika można skonfigurować następujące parametry:

- dla serwera Acronis Backup & Recovery 11 Management Server: **Collecting Logs, Windows Event Log, SNMP, SNMP Address, SNMP Community** oraz **Online Backup**
- dla komponentu Acronis Backup & Recovery 11 Agent: **Windows Event Log, SNMP, SNMP Address, SNMP Community, Customer Experience Program** oraz **Online Backup**

Opis poszczególnych parametrów można znaleźć w odpowiednim temacie dotyczącym konfiguracji przy użyciu szablonu administracyjnego.

12 Słownik

A

Acronis Active Restore

Technologia Acronis przywracająca połączenie internetowe niezwłocznie po rozpoczęciu odzyskiwania systemu. Komputer działa i udostępnia niezbędne usługi po uruchomieniu systemu z kopii zapasowej (s. 381). Najwyższy priorytet ma odzyskiwanie danych umożliwiających obsługę żądań przychodzących. Reszta danych jest odzyskiwana w tle. Ograniczenia:

- kopia zapasowa musi znajdować się na dysku lokalnym (dowolnym urządzeniu dostępnym z systemu BIOS, z wyjątkiem urządzenia uruchamianego przez sieć);
- nie działa z obrazami systemu Linux.

Acronis Plug-in for WinPE

Zmodyfikowana wersja komponentu Acronis Backup & Recovery 11 Agent for Windows, którą można uruchomić w środowisku przedinstalacyjnym. Wtyczkę można dodać do obrazu WinPE (s. 387) przy użyciu programu Generator nośnika startowego. Otrzymany nośnik startowy (s. 381) może służyć do uruchamiania dowolnego komputera klasy PC i umożliwia wykonywanie (z pewnymi ograniczeniami) większości operacji zarządzania bezpośredniego (s. 389) bez potrzeby korzystania z systemu operacyjnego. Operacje można konfigurować i nadzorować lokalnie za pośrednictwem graficznego interfejsu użytkownika lub zdalnie przy użyciu konsoli (s. 380).

Acronis Startup Recovery Manager (ASRM)

Zmodyfikowana wersja agenta startowego (s. 376), znajdująca się na dysku systemowym i uruchamiana po naciśnięciu klawisza F11 podczas uruchamiania komputera. Program Acronis Startup Recovery Manager eliminuje potrzebę użycia nośnika ratunkowego lub połączenia sieciowego w celu uruchomienia ratunkowego narzędzia startowego.

Acronis Startup Recovery Manager jest szczególnie przydatny dla użytkowników urządzeń przenośnych. W razie awarii należy ponownie uruchomić komputer, nacisnąć klawisz F11 po wyświetleniu monitu „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager...” oraz odzyskać dane w taki sam sposób jak ze zwykłego nośnika startowego.

Ograniczenie: wymaga ponownej aktywacji programów ładujących (nie dotyczy programu ładującego systemu Windows i GRUB).

Acronis Universal Restore

Zastrzeżona technologia firmy Acronis, która ułatwia uruchamianie systemu Windows lub Linux na sprzęcie o innej konfiguracji lub na maszynie wirtualnej. Funkcja Universal Restore niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu operacyjnego, takimi jak kontrolery pamięci, płyta główna i chipset.

Funkcja Universal Restore jest niedostępna, gdy:

- następuje umiejscowienie odzyskiwanego obrazu w strefie Acronis Secure Zone (s. 386),
- jest używana funkcja Acronis Active Restore (s. 375),

ponieważ są to funkcje przeznaczone głównie do błyskawicznego odzyskiwania danych na tym samym komputerze.

Agent (Acronis Backup & Recovery 11 Agent)

Aplikacja do tworzenia kopii zapasowej danych i ich odzyskiwania oraz umożliwiająca wykonywanie innych operacji zarządzania na komputerze (s. 380), takich jak zarządzanie zadaniami i operacje na dysku twardym.

Typ danych, których kopię zapasową można utworzyć, zależy od typu agenta. Acronis Backup & Recovery 11 zawiera agenty do tworzenia kopii zapasowych dysków i plików oraz agenty do tworzenia kopii zapasowych maszyn wirtualnych znajdujących się na serwerach wirtualizacji.

Agent startowy

Ratunkowe narzędzie startowe z większością funkcji agenta Acronis Backup & Recovery 11 Agent (s. 376). Agent startowy korzysta z jądra systemu Linux. Komputer (s. 380) można uruchomić w agencie startowym przy użyciu nośnika startowego (s. 381) lub serwera Acronis PXE Server. Operacje można konfigurować i kontrolować lokalnie za pośrednictwem graficznego interfejsu użytkownika lub zdalnie przy użyciu konsoli (s. 380).

Archiwum

Zobacz Archiwum kopii zapasowej (s. 376).

Archiwum kopii zapasowej (Archiwum)

Zestaw kopii zapasowych (s. 380) tworzonych i zarządzanych przez plan tworzenia kopii zapasowych (s. 382). W archiwum może się znajdować wiele pełnych kopii zapasowych (s. 382), a także kopii przyrostowych (s. 383) i różnicowych (s. 384). Kopie zapasowe należące do tego samego archiwum są zawsze przechowywane w tej samej lokalizacji. Jeśli plan tworzenia kopii zapasowych obejmuje replikację (s. 384) lub przenoszenie kopii zapasowych do wielu lokalizacji, kopie zapasowe w każdej z takich lokalizacji tworzą odrębne archiwum.

Archiwum zaszyfrowane

Archiwum kopii zapasowej (s. 376) zaszyfrowane przy użyciu algorytmu Advanced Encryption Standard (AES). Jeśli opcja szyfrowania oraz hasło archiwum są ustawiane w opcjach tworzenia kopii zapasowej (s. 382), każda kopia zapasowa w ramach danego archiwum jest szyfrowana przez agenta (s. 376) przed jej zapisem w miejscu docelowym.

C

Czyszczenie

Usuwanie kopii zapasowych (s. 380) z archiwum kopii zapasowych (s. 376) lub przenoszenie ich do innej lokalizacji w celu pozbycia się nieaktualnych kopii lub zapobieżenia przekroczeniużądanego rozmiaru archiwum.

Czyszczenie polega nastosowaniu reguł przechowywania (s. 383) w odniesieniu do archiwum. Reguły przechowywania są ustalane przez plan tworzenia kopii zapasowych (s. 382), w wyniku którego powstaje archiwum. Czyszczenie może spowodować usunięcie lub przeniesienie kopii zapasowych w zależności od tego, czy zostaną przekroczone określone reguły przechowywania.

D

Deduplikacja

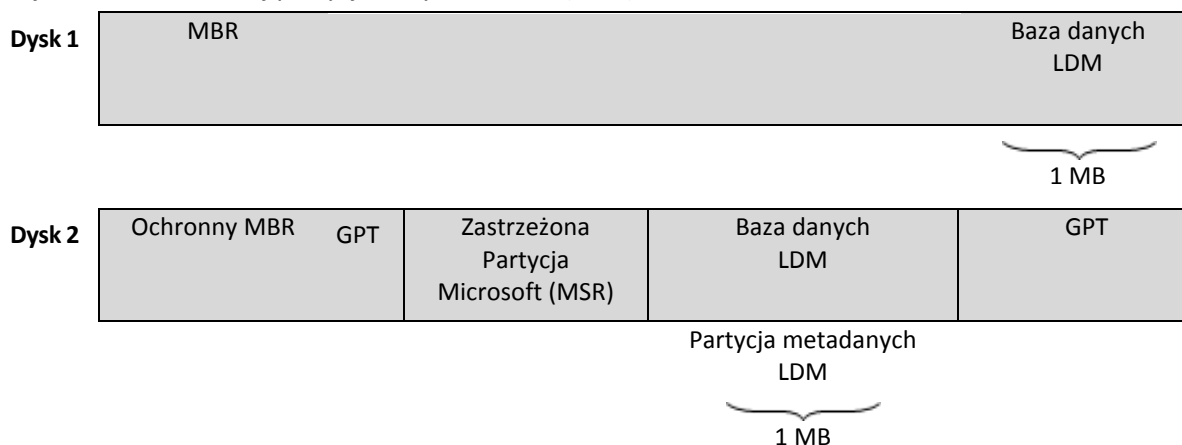
Metoda umożliwiająca zapis wielu duplikatów tej samej informacji tylko jeden raz.

Produkt Acronis Backup & Recovery 11 umożliwia stosowanie technologii deduplikacji w archiwach kopii zapasowych (s. 376) przechowywanych w węzłach magazynowania (s. 386). Minimalizuje ona ilość miejsca zajmowanego przez archiwa oraz ruch sieciowy i wykorzystanie sieci podczas tworzenia kopii zapasowej.

Dysk dynamiczny

Dysk twardy zarządzany przez Menedżera dysków logicznych (LDM), który jest dostępny w systemach Windows, począwszy od Windows 2000. LDM ułatwia elastyczne przydzielanie woluminów na urządzeniu pamięci w celu uzyskania wyższej odporności na uszkodzenia, wyższej wydajności lub większego rozmiaru woluminu.

Dysk dynamiczny może korzystać z głównego rekordu rozruchowego (MBR) lub stylu partycjonowania GPT z tabelą partycji GUID. Poza rekordem MBR lub stylem GPT na każdym dysku dynamicznych znajduje się ukryta baza danych, w której usługa LDM przechowuje informacje o konfiguracji woluminów dynamicznych. Na każdym dysku dynamicznym znajdują się pełne informacje o wszystkich woluminach dynamicznych istniejących w grupie dysków, co zapewnia większą niezawodność magazynu. Baza danych zajmuje przynajmniej 1 MB miejsca na dysku MBR. Na dysku GPT system Windows tworzy dedykowaną partycję metadanych usługi LDM, rezerwując dla niej miejsce na zastrzeżonej partycji firmy Microsoft (MSR).



Dyski dynamiczne są zorganizowane na dyskach MBR (dysk 1) i GPT (dysk 2).

Aby uzyskać więcej informacji na temat dysków dynamicznych, zobacz następujące artykuły bazy wiedzy Microsoft Knowledge Base:

Disk Management (Windows XP Professional Resource Kit) <http://technet.microsoft.com/en-us/library/bb457110.aspx>.

816307 Best practices for using dynamic disks on Windows Server 2003-based computers <http://support.microsoft.com/kb/816307/pl>.

Dziadek-ojciec-syn (GFS)

Popularny schemat tworzenia kopii zapasowych (s. 384) mający na celu zachowanie optymalnej proporcji między rozmiarem archiwum kopii zapasowej (s. 376) a liczbą punktów odzyskiwania (s. 383) dostępnych w archiwum. GFS umożliwia codzienne odzyskiwanie danych z ostatnich siedmiu dni, cotygodniowe — danych z ostatnich kilku tygodni oraz comiesięczne — danych z dowolnej chwili w przeszłości.

Aby uzyskać więcej informacji na ten temat, zobacz Schemat tworzenia kopii zapasowych dziadek-ojciec-syn.

Działanie

Działanie wykonywane przez program Acronis Backup & Recovery 11 dla osiągnięcia celu założonego przez użytkownika. Przykłady: tworzenie kopii zapasowej, odzyskiwanie, eksportowanie kopii zapasowej, katalogowanie skarbca. Działanie może zainicjować użytkownik lub sam program. Realizacja zadania (s. 388) zawsze powoduje wykonanie jednego lub więcej działań.

E

Eksportuj

Operacja, która tworzy kopię archiwum (s. 376) lub samowystarczalną częściową kopię archiwum w określonej lokalizacji. Operacja eksportu może być zastosowana do jednego archiwum, jednej kopii zapasowej (s. 380) lub do wielu wybranych kopii należących do tego samego archiwum. Za pomocą interfejsu wiersza poleceń można wykonać eksport całego skarbca (s. 385).

G

Generator nośnika

Dedykowane narzędzie do tworzenia nośnika startowego (s. 381).

Grupa dynamiczna

Grupa komputerów (s. 380) uzupełniana automatycznie przez serwer zarządzania (s. 384) zgodnie z kryteriami członkostwa, które określił administrator. Program Acronis Backup & Recovery 11 udostępnia następujące kryteria członkostwa:

- System operacyjny,
- Jednostka organizacyjna usługi Active Directory
- Zakres adresów IP
- Lista w pliku txt/csv.

Komputer pozostaje w grupie dynamicznej tak długo, jak długo spełnia określone w niej kryteria członkostwa. Administrator może jednak określić wykluczenia pozwalające na nieuwzględnienie niektórych komputerów w grupie dynamicznej, nawet jeśli spełniają jej kryteria.

Grupa dysków

Określona liczba dysków dynamicznych (s. 377) do przechowywania typowych danych konfiguracyjnych w bazach danych LDM, którymi można zarządzać jako całością. Zwykle wszystkie dyski dynamiczne utworzone na tym samym komputerze (s. 380) należą do tej samej grupy dysków.

Po utworzeniu pierwszego dysku dynamicznego w LDM lub innym narzędziu do zarządzania dyskami nazwa grupy dysków pojawi się w kluczu rejestru
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name.

Kolejne tworzone lub importowane dyski zostaną dodane do tej samej grupy dysków. Grupa istnieje dopóki istnieje przynajmniej jeden jej członek. Po odłączeniu ostatniego dysku dynamicznego lub skonwertowaniu go na dysk podstawowy grupa przestaje istnieć, ale jej nazwa pozostaje w kluczu rejestru podanym powyżej. Po ponownym utworzeniu lub podłączeniu dysku dynamicznego zostanie utworzona grupa dysków o nazwie przyrostowej.

Po przeniesieniu grupy dysków na inny komputer jest ona obsługiwana jako „obca” i nie można z niej korzystać dopóki nie zostanie zaimportowana do istniejącej grupy dysków. Import spowoduje aktualizację danych konfiguracyjnych zarówno na dyskach lokalnych, jak i obcych, dzięki czemu będą one tworzyć jedną grupę. Jeśli na komputerze nie istnieje żadna grupa dysków, grupa obca zostanie zaimportowana w aktualnej postaci (z oryginalną nazwą).

Aby uzyskać więcej informacji na temat grup dysków, zobacz następujący artykuł bazy wiedzy Microsoft Knowledge Base:

222189 Description of Disk Groups in Windows Disk Management
<http://support.microsoft.com/kb/222189/pl-pl/>.

Grupa statyczna

Grupa komputerów, które administrator serwera zarządzania (s. 384) wypełnia ręcznie, dodając je do grupy. Komputer pozostanie w grupie statycznej dopóki administrator nie usunie go z tej grupy lub z serwera zarządzania.

Grupa wbudowana

Grupa komputerów zawsze znajdująca się na serwerze zarządzania (s. 384).

Grupy wbudowane nie mogą być usuwane, przenoszone do innych grup ani ręcznie modyfikowane. W ich ramach nie można tworzyć grup niestandardowych. Jedynym sposobem usunięcia komputera z grupy wbudowanej jest usunięcie go z serwera zarządzania.



Indeksowanie

Działanie (s. 378) wykonywane przez węzeł magazynowania (s. 386) po zapisaniu kopii zapasowej (s. 380) w skarbcu deduplikacji (s. 385).

Podczas indeksowania węzeł magazynowania wykonuje następujące operacje:

- Przenosi bloki danych z kopii zapasowej do specjalnego pliku w skarbcu. Plik ten nazywany jest magazynem danych deduplikacji.
- Zamienia przeniesione bloki w kopii zapasowej na ich odciski („skrót”).
- Zapisuje w bazie danych deduplikacji wartości skrótów i łączy niezbędne do „złożenia” danych po deduplikacji.

Indeksowanie można rozumieć jako „deduplikację w miejscu docelowym” w odróżnieniu od „deduplikacji w miejscu źródłowym” wykonywanej przez agenta (s. 376) w trakcie operacji tworzenia kopii zapasowej (s. 382). Użytkownik może wstrzymywać i wznowiać indeksowanie.

K

Katalogowanie

Katalogowanie kopii zapasowej (s. 380) powoduje dodanie jej zawartości do wykazu danych (s. 388). Kopie zapasowe są automatycznie katalogowane przez agenta (s. 376) zaraz po ich utworzeniu. Użytkownik może wyłączyć funkcję automatycznego katalogowania i uruchamiać ją ręcznie w dogodnym czasie. Kopie zapasowe przechowywane w węźle magazynowania (s. 386) będą w takim przypadku katalogowane przez węzeł.

Komputer

Komputer fizyczny lub wirtualny o unikalnym identyfikatorze uzyskanym podczas instalacji systemu operacyjnego. Komputery z wieloma systemami operacyjnymi są obsługiwane jak wiele komputerów.

Komputer zarejestrowany

Komputer (s. 380) zarządzany przez serwer zarządzania (s. 384). Komputer można zarejestrować tylko na jednym serwerze zarządzania naraz. Komputer zostanie zarejestrowany w wyniku wykonania procedury rejestracji (s. 383).

Komputer zarządzany

Komputer (s. 380) fizyczny lub wirtualny, na którym jest zainstalowany co najmniej jeden agent Acronis Backup & Recovery 11 (s. 376).

Konsola (Acronis Backup & Recovery 11 Management Console)

Narzędzie umożliwiające dostęp zdalny lub lokalny do agentów Acronis (s. 376) i serwera Acronis Backup & Recovery 11 Management Server (s. 384).

Po podłączeniu konsoli do serwera zarządzania administrator konfiguruje scentralizowane plany tworzenia kopii zapasowych (s. 384) i ma dostęp do innych funkcji serwera zarządzania, tj. prowadzi zarządzanie scentralizowane (s. 389). Przy użyciu bezpośredniego połączenia konsola-agent administrator prowadzi zarządzanie bezpośrednie (s. 389).

Konsolidacja

Scalenie dwóch lub więcej kolejnych kopii zapasowych (s. 380) z tego samego archiwum (s. 376) w jedną kopię zapasową.

Konsolidacja może być wymagana przy usuwaniu kopii zapasowych, zarówno ręcznym, jak i wykonywanym podczas czyszczenia (s. 376). Na przykład reguły przechowywania określają, że jest wymagane usunięcie nieaktualnej pełnej kopii zapasowej (s. 382), ale należy pozostawić kolejną kopię przyrostową (s. 383). Kopie zapasowe zostaną scalone w jedną pełną kopię zapasową, której datą utworzenia będzie data utworzenia przyrostowej kopii zapasowej. Konsolidacja może zająć dużo czasu i korzystać z dużej ilości zasobów, dlatego w regułach przechowywania istnieje opcja nieusuwania kopii zapasowych z zależnościami. W podanym przykładzie pełna kopia zapasowa będzie istnieć aż do czasu, gdy przyrostowa kopia zapasowa stanie się również nieaktualna. Wtedy obie kopie zapasowe zostaną usunięte.

Kopia zapasowa

Kopia zapasowa to wynik pojedynczej operacji tworzenia kopii zapasowej (s. 382). W ujęciu fizycznym jest to plik lub zapis na taśmie zawierający kopię zapasową danych wykonaną w określonym dniu o określonej godzinie. Pliki kopii zapasowych utworzone w programie Acronis Backup & Recovery 11 mają rozszerzenie TIB. Również pliki TIB powstałe w wyniku wyeksportowania (s. 378) lub konsolidacji (s. 380) kopii zapasowych są nazywane kopiami zapasowymi.

Kopia zapasowa (obraz) dysku

Kopia zapasowa (s. 380) „sektor po sektorze” dysku lub woluminu w postaci spakowanej. Zwykle są kopiowane tylko sektory zawierające dane. Produkt Acronis Backup & Recovery 11 udostępnia opcję utworzenia obrazu nieprzetworzonych danych, czyli skopiowania wszystkich sektorów dysku, dzięki czemu można uzyskać obraz nieobsługiwanych systemów plików.

L

Lokalny plan tworzenia kopii zapasowych

Plan tworzenia kopii zapasowych (s. 382) utworzony na komputerze zarządzanym (s. 380) przy użyciu zarządzania bezpośredniego (s. 389).

M

Maszyna wirtualna

Na serwerze zarządzania Acronis Backup & Recovery 11 Management Server (s. 384) komputer (s. 380) jest traktowany jako maszyna wirtualna, jeśli można wykonać jego kopię zapasową z hosta wirtualizacji, nie instalując na nim agenta (s. 376). Taki komputer występuje w sekcji **Maszyny wirtualne**. W przypadku instalacji agenta w systemie gościa komputer taki znajduje się w sekcji **Komputery z agentami**.

N

Nośnik startowy

Nośnik fizyczny (płyta CD lub DVD, dysk flash USB albo inny nośnik obsługiwany jako urządzenie startowe w systemie BIOS komputera (s. 380)), który zawiera agenta startowego (s. 376) lub środowisko preinstalacyjne systemu Windows (WinPE) (s. 387) z wtyczką Acronis Plug-in for WinPE (s. 375). Komputer można również uruchomić w powyższych środowiskach przy użyciu funkcji uruchamiania przez sieć z serwera Acronis PXE Server lub za pomocą usługi Windows Deployment Service (WDS). Takie serwery z przesłanymi komponentami startowymi można również traktować jako swego rodzaju nośniki startowe.

Najczęstsze zastosowanie nośnika startowego:

- odzyskiwanie systemu operacyjnego, którego nie można uruchomić;
- uzyskanie dostępu do danych ocalałych w uszkodzonym systemie i utworzenie ich kopii zapasowej;
- wdrożenie systemu operacyjnego po awarii;
- tworzenie woluminów standardowych lub dynamicznych (s. 387) od zera (ang. bare metal);
- utworzenie kopii zapasowej „sektor po sektorze” dysku z nieobsługiwany systemem plików;

- utworzenie w trybie offline kopii zapasowej wszelkich danych, których kopii zapasowej nie można utworzyć w trybie online ze względu na ograniczony dostęp, trwałą blokadę założoną przez uruchomione aplikacje lub z jakichkolwiek innych powodów.

O

Obraz

To samo, co kopia zapasowa dysku (s. 381).

Opcje tworzenia kopii zapasowych

Parametry konfiguracyjne operacji tworzenia kopii zapasowej (s. 382), takie jak polecenia poprzedzające tworzenie kopii zapasowej/następujące po nim, maksymalna przepustowość sieci przydzielona do strumienia kopii zapasowej lub poziom kompresji danych. Opcje tworzenia kopii zapasowych są częścią planu tworzenia kopii zapasowych (s. 382).

Operacja tworzenia kopii zapasowej

Operacja powodująca utworzenie kopii danych znajdujących się na dysku twardym komputera (s. 380) w celu odzyskania danych lub przywrócenia ich z określonego dnia i godziny.

P

Pełna kopia zapasowa

Samowystarczalna kopia zapasowa (s. 380) zawierająca wszystkie dane wybrane przy tworzeniu kopii zapasowej. Odzyskanie danych z pełnej kopii zapasowej nie wymaga dostępu do żadnej innej kopii zapasowej.

Plan

Zobacz Plan tworzenia kopii zapasowych (s. 382).

Plan odzyskiwania po awarii (DRP)

Wiadomość e-mail zawierająca listę elementów danych znajdujących się w kopii zapasowej oraz szczegółowe instrukcje dotyczące sposobu ich odzyskania.

Jeśli odpowiednia opcja tworzenia kopii zapasowej (s. 382) jest włączona, wiadomość DRP jest wysyłana na określone adresy e-mail po pierwszym pomyślnym utworzeniu kopii zapasowej w ramach planu oraz w przypadku każdej zmiany listy elementów danych lub parametrów DRP.

Plan tworzenia kopii zapasowych (Plan)

Zestaw reguł określających sposób ochrony konkretnych danych na konkretnym komputerze. Parametry określane w planie tworzenia kopii zapasowych:

- dane uwzględniane w kopii zapasowej;
- nazwa i lokalizacja archiwum kopii zapasowej (s. 376);
- schemat tworzenia kopii zapasowych (s. 384). Obejmuje on harmonogram kopii zapasowych oraz [opcjonalnie] reguły przechowywania (s. 383)

- [opcjonalnie] dodatkowe operacje, które należy wykonać wraz z tworzeniem kopii zapasowych (replikacja (s. 384), sprawdzanie poprawności (s. 386), konwersja na maszynę wirtualną)
- opcje tworzenia kopii zapasowych (s. 382).

Na przykład w planie tworzenia kopii zapasowych mogą się znajdować następujące informacje:

- utworzyć kopię zapasową woluminu C: **(te dane zostaną objęte ochroną planu)**;
- nadać archiwum nazwę MójWoluminSystemowy i umieścić je w folderze \\serwer\kopiezapasowe\ **(są to nazwa i lokalizacja archiwum kopii zapasowej)**;
- stworzyć pełną kopię zapasową co miesiąc w ostatni dzień miesiąca o godzinie 10:00 oraz przyrostową kopię zapasową w każdą niedzielę o godzinie 22:00; usuwać kopie zapasowe starsze niż 3 miesiące **(jest to schemat tworzenia kopii zapasowych)**;
- sprawdzić poprawność ostatniej kopii zapasowej niezwłocznie po jej utworzeniu **(jest to reguła sprawdzania poprawności)**;
- chronić archiwum hasłem **(jest to ustawienie opcjonalne)**.

W ujęciu fizycznym plan tworzenia kopii zapasowych to pakiet zadań (s. 388) wykonywanych na komputerze zarządzanym (s. 380).

Plan tworzenia kopii zapasowych może powstać bezpośrednio na komputerze, którego dotyczy, może zostać zaimportowany z innego komputera (plan lokalny) lub przekazany do komputera z serwera zarządzania (plan scentralizowany (s. 384)).

Przyrostowa kopia zapasowa

Kopia zapasowa (s. 380) do przechowywania danych, które zostały zmienione od czasu tworzenia ostatniej kopii zapasowej. Aby odzyskać dane z przyrostowej kopii zapasowej, należy uzyskać dostęp do innych kopii zapasowych z tego samego archiwum (s. 376).

Pula uzupełnialna

Pula taśm, która może w razie potrzeby pobierać taśmy z puli **Wolne taśmy**.

Punkt odzyskiwania

Data i godzina utworzenia kopii zapasowej danych, które można przywrócić.

R

Reguły przechowywania

Część planu tworzenia kopii zapasowych (s. 382) określająca czas i sposób usuwania lub przenoszenia kopii zapasowych (s. 380) utworzonych w ramach planu.

Rejestracja

Procedura umożliwiająca dodanie komputera zarządzanego (s. 380) do serwera zarządzania (s. 384).

Rejestracja polega na utworzeniu relacji zaufania między agentami (s. 376) znajdującymi się na komputerze i serwerze. Podczas rejestracji konsola pobiera certyfikat kliencki serwera zarządzania i przekazuje go do agenta, który użyje go później do uwierzytelnienia klientów nawiązujących połączenie. Dzięki temu można zapobiec wszelkim próbom ataków sieciowych polegających na

ustanowieniu fałszywego połączenia w imieniu zaufanego podmiotu zabezpieczeń (serwera zarządzania).

Replikacja

Kopiowanie kopii zapasowej (s. 380) do innej lokalizacji. Domyślnie kopia zapasowa jest kopiowana niezwłocznie po utworzeniu. Użytkownik ma możliwość odroczenia tego procesu, konfigurując czas braku aktywności replikacji.

Funkcja ta zastąpiła funkcję tworzenia kopii zapasowej w dwóch miejscach docelowych dostępną w programie Acronis Backup & Recovery 10, zapewniając większą elastyczność działania.

Różnicowa kopia zapasowa

W różnicowej kopii zapasowej są zapisywane dane, które zostały zmienione od czasu utworzenia ostatniej pełnej kopii zapasowej (s. 382). Aby odzyskać dane z różnicowej kopii zapasowej, należy uzyskać dostęp do odpowiedniej pełnej kopii zapasowej.

S

Scentralizowany plan tworzenia kopii zapasowych

Plan tworzenia kopii zapasowych (s. 382) wdrożony na komputerze zarządzanym (s. 380) z poziomu serwera zarządzania (s. 384). Plan taki można modyfikować jedynie w drodze edycji oryginalnego planu tworzenia kopii zapasowych na serwerze zarządzania.

Schemat tworzenia kopii zapasowych

Część planu tworzenia kopii zapasowych (s. 382) obejmująca harmonogram tworzenia kopii zapasowych oraz (opcjonalnie) reguły przechowywania i harmonogram czyszczenia (s. 376). Na przykład: twórz pełną kopię zapasową (s. 382) co miesiąc w ostatni dzień miesiąca o godzinie 10:00 oraz przyrostową kopię zapasową (s. 383) w każdą niedzielę o godzinie 22:00. Usuń kopie zapasowe starsze niż 3 miesiące. Sprawdź obecność takich kopii po ukończeniu każdej operacji tworzenia kopii zapasowej.

Program Acronis Backup & Recovery 11 udostępnia dobrze znane, zoptymalizowane schematy tworzenia kopii zapasowych, takie jak GFS i Wieża Hanoi, przy użyciu których można opracowywać własne schematy tworzenia kopii zapasowych lub jednorazowo tworzyć kopie zapasowe danych.

Serwer zarządzania (Acronis Backup & Recovery 11 Management Server)

Centralny serwer sterujący ochroną danych w sieci przedsiębiorstwa. Serwer zarządzania Acronis Backup & Recovery 11 Management Server zapewnia administratorowi:

- jeden punkt wejścia do infrastruktury Acronis Backup & Recovery 11;
- łatwy sposób ochrony danych na wielu komputerach (s. 380) przy użyciu scentralizowanych planów tworzenia kopii zapasowych (s. 384) i możliwości ich grupowania;
- funkcje monitorowania obejmujące całe przedsiębiorstwo;
- możliwość tworzenia skarbów centralnych (s. 385) do przechowywania archiwów kopii zapasowych (s. 376) przedsiębiorstwa;
- możliwość zarządzania węzłami magazynowania (s. 386);
- scentralizowany wykaz (s. 388) wszystkich danych przechowywanych w węzłach magazynowania.

Jeśli w sieci istnieje wiele serwerów zarządzania, działają one niezależnie, zarządzają innymi komputerami i korzystają z innych skarbów centralnych do przechowywania archiwów.

Skarbiec

Miejsce do zachowywania archiwów kopii zapasowych (s. 376). Skarbiec można zorganizować na dysku lokalnym lub sieciowym albo nośniku wymiennym, takim jak zewnętrzny dysk USB. Nie istnieją ustawienia umożliwiające ograniczenie rozmiaru skarbca ani liczby kopii zapasowych w skarbcu. Rozmiar każdego archiwum można ograniczyć, korzystając z funkcji czyszczenia (s. 376), ale całkowity rozmiar archiwów przechowywanych w skarbcu jest ograniczony tylko rozmiarem magazynu.

Skarbiec centralny

Lokalizacja sieciowa przydzielona przez administratora serwera zarządzania (s. 384) jako miejsce przechowywania archiwów kopii zapasowych (s. 376). Skarbiec centralny może być zarządzany przez węzeł magazynowania (s. 386) lub niezarządzany. Całkowita liczba i rozmiar archiwów przechowywanych w skarbcu centralnym są ograniczone jedynie wielkością dostępnej pamięci masowej.

Gdy administrator serwera zarządzania utworzy skarbiec centralny, nazwa i ścieżka do skarbca są niezwłocznie rozsyłane do wszystkich komputerów zarejestrowanych (s. 380) na serwerze. Na liście **Skarbce** na komputerach pojawia się skrót do nowego skarbca. Ze skarbca centralnego mogą korzystać dowolne plany tworzenia kopii zapasowych (s. 382) istniejące na komputerach, w tym plany lokalne.

Na komputerze, który nie jest zarejestrowany na serwerze zarządzania, użytkownik mający uprawnienia do tworzenia kopii zapasowych w skarbcu centralnym może wykonać te czynności, określając pełną ścieżkę do skarbca. Jeśli skarbiec jest zarządzany, węzeł magazynowania umożliwi zarządzanie archiwami użytkownika podobnie jak innymi archiwami przechowywanymi w skarbcu.

Skarbiec deduplikacji

Skarbiec zarządzany (s. 385), w którym można wykonać deduplikację (s. 376).

Skarbiec niezarządzany

Każdy skarbiec (s. 385), który nie jest skarbcem zarządzanym (s. 385).

Skarbiec osobisty

Lokalny lub sieciowy skarbiec (s. 385) utworzony przy użyciu funkcji zarządzania bezpośredniego (s. 389). Po utworzeniu skarbca osobistego skrót do niego zostanie wyświetlony na komputerze zarządzanym na liście **Skarbce**. Rolę skarbca osobistego w odniesieniu do różnych komputerów może pełnić ta sama lokalizacja fizyczna, na przykład dysk sieciowy.

Skarbiec zarządzany

Skarbiec centralny (s. 385) zarządzany przez węzeł magazynowania (s. 386). Archiwa (s. 376) w skarbcu zarządzanym są dostępne za pomocą następującego adresu:

`bsp://adres_węzła/nazwa_skarbca/nazwa_archiwum/`

Skarbcze zarządzane mogą się fizycznie znajdować w udziale sieciowym, systemie SAN, udziale NAS, na lokalnym dysku twardym węzła magazynowania lub w bibliotece taśm podłączonej lokalnie do węzła magazynowania. Węzeł magazynowania wykonuje zadania czyszczenia (s. 376) oraz sprawdzania poprawności (s. 386) w odniesieniu do każdego archiwum przechowywanego z skarbcu zarządzanym. Administrator może określać dodatkowe operacje, które ma wykonywać węzeł magazynowania (takie jak deduplikacja (s. 376) czy szyfrowanie).

Skarbiec zaszyfrowany

Skarbiec zarządzany (s. 385), w którym wszystkie zapisywane dane są szyfrowane, a wszystkie odczytywane dane są deszyfrowane w czasie rzeczywistym przez węzeł magazynowania (s. 386) przy użyciu klucza szyfrowania skarbcza przechowywanego w tym węźle. W przypadku kradzieży nośnika magazynu lub uzyskania do niego dostępu przez osobę nieautoryzowaną odszyfrowanie zawartości skarbcza bez dostępu do węzła magazynowania będzie niemożliwe. Archiwa zaszyfrowane (s. 376) będą zaszyfrowane przez agenta (s. 376).

Sprawdzanie poprawności

Operacja sprawdzająca, czy można odzyskać dane z kopii zapasowej (s. 380).

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. Obie procedury intensywnie wykorzystują zasoby komputera.

Pomyślny wynik sprawdzania poprawności oznacza wysokie prawdopodobieństwo poprawnego odzyskania danych, ale kontrola taka nie obejmuje weryfikacji wszystkich czynników wpływających na proces odzyskiwania. W przypadku kopii zapasowej systemu operacyjnego jedynie odzyskiwanie testowe za pomocą nośnika startowego na zapasowy dysk twardy może dać gwarancję pomyślnego odzyskiwania w przyszłości.

Strefa Acronis Secure Zone

Bezpieczny wolumin do przechowywania archiwów (s. 376) kopii zapasowych na komputerze zarządzanym (s. 380). Zalety:

- umożliwia odzyskanie zawartości dysku na ten sam dysk, na którym znajduje się jego kopia zapasowa;
- tania i przydatna metoda ochrony danych przed nieprawidłowym działaniem oprogramowania, atakiem wirusów, błędem operatora;
- eliminuje potrzebę użycia dodatkowego nośnika lub połączenia sieciowego w celu utworzenia kopii zapasowej lub odzyskania danych. Jest to szczególnie przydatne dla użytkowników urządzeń mobilnych;
- może służyć jako podstawowa lokalizacja, z której następuje dalsza replikacja kopii zapasowych.

Ograniczenie: Strefy Acronis Secure Zone nie można zorganizować na dysku dynamicznym (s. 377).

Strefa Acronis Secure Zone jest obsługiwana jako skarbiec osobisty (s. 385).

W

Węzeł magazynowania (Acronis Backup & Recovery 11 Storage Node)

Serwer zaprojektowany do optymalnego korzystania z różnych zasobów wymaganych do ochrony danych w przedsiębiorstwie. Cel ten osiąga się dzięki zakładaniu skarbców zarządzanych (s. 385). Zalety węzła magazynowania z punktu widzenia administratora:

- użycie pojedynczego, scentralizowanego wykazu (s. 388) danych przechowywanych w skarbcach zarządzanych;
- zwolnienie komputerów zarządzanych (s. 380) z wykonywania wymagających intensywnej pracy procesora zadań czyszczenia (s. 376), sprawdzania poprawności (s. 386) oraz innych operacji dotyczących archiwów kopii zapasowych (s. 376), które w innym przypadku byłby wykonywane przez agenty (s. 376);
- poważne zmniejszenie ruchu związanego z kopiami zapasowymi oraz ilości miejsca zajmowanego w magazynie przez archiwa (s. 376) dzięki zastosowaniu deduplikacji (s. 376);
- uniemożliwienie dostępu do archiwów kopii zapasowych nawet w przypadku kradzieży nośnika danych lub uzyskania do niego dostępu przez osobę nieuprawnioną — dzięki użyciu skarbców zaszyfrowanych (s. 386).

Wieża Hanoi

Popularny schemat tworzenia kopii zapasowych (s. 384) mający na celu zachowanie optymalnej proporcji między rozmiarem archiwum kopii zapasowej (s. 376) a liczbą punktów odzyskiwania (s. 383) dostępnych w archiwum. W odróżnieniu od schematu dziadek-ojciec-syn (s. 377) mającego tylko trzy poziomy odzyskiwania (codziennie, co tydzień, co miesiąc), schemat Wieża Hanoi wraz ze zwiększaniem się wieku kopii zapasowej stale zmniejsza interwał czasu między kolejnymi punktami odzyskiwania. Dzięki temu można bardzo efektywnie korzystać z magazynu kopii zapasowych.

Aby uzyskać więcej informacji na ten temat, zobacz „Schemat tworzenia kopii zapasowych — Wieża Hanoi (s. 62)”.

WinPE (Środowisko preinstalacyjne systemu Windows)

Minimalna wersja systemu Windows wykorzystująca jedno z następujących jąder:

- Windows XP Professional z dodatkiem Service Pack 2 (PE 1.5);
- Windows Server 2003 z dodatkiem Service Pack 1 (PE 1.6);
- Windows Vista (PE 2.0);
- Windows Vista SP1 i Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0).

Środowisko WinPE jest często wykorzystywane przez producentów OEM i korporacje do wdrażania, testowania, diagnostyki i naprawy systemów. Środowisko WinPE można uruchomić na komputerze za pomocą serwera PXE, płyty CD-ROM, dysku flash USB lub dysku twardego. Wtyczka Acronis Plug-in for WinPE (s. 375) umożliwia uruchomienie komponentu Acronis Backup & Recovery 11 Agent (s. 376) w środowisku preinstalacyjnym.

Wolumin dynamiczny

Dowolny wolumin znajdujący się na dyskach dynamicznych (s. 377), a dokładniej — w grupie dysków (s. 378). Woluminy dynamiczne mogą zajmować wiele dysków i są zwykle skonfigurowane w zależności od celu ich utworzenia:

- zwiększenie rozmiaru woluminu (wolumin łączony);
- skrócenie czasu dostępu (wolumin rozłożony);
- uzyskanie odporności na uszkodzenia przez wprowadzenie nadmiarowości (woluminy lustrzane i RAID-5).

Wolumin logiczny

To pojęcie ma dwa znaczenia, w zależności od kontekstu.

- Wolumin, informacje o którym są zapisane w tablicy partycji rozszerzonej. (W odróżnieniu od woluminu podstawowego, informacje o którym są przechowywane w głównym rekordzie startowym).
- Wolumin utworzony za pomocą menedżera woluminów logicznych (LVM) dla jądra systemu Linux. Menedżer LVM daje administratorowi możliwość elastycznej redystrybucji na żądanie dużych ilości miejsca do przechowywania danych oraz dodawania nowych i usuwania starych dysków fizycznych bez przerywania usług użytkownika. Komponent Acronis Backup & Recovery 11 Agent (s. 376) for Linux umożliwia dostęp do woluminów logicznych, tworzenie ich kopii zapasowych oraz ich odzyskiwanie w systemie Linux z jądrem 2.6.x lub przy użyciu nośnika startowego (s. 381) opartego na systemie Linux.

Wykaz danych

Wykaz danych ułatwia wyszukiwanie wymaganej wersji danych i wybranie ich do odzyskania. Użytkownicy komputera zarządzanego (s. 380) mogą przeglądać i przeszukiwać dane zgromadzone w każdym skarbcu (s. 385) dostępnym z tego komputera. Katalog scentralizowany dostępny na serwerze zarządzania (s. 384) zawiera wszystkie dane zapisane w jego węzłach magazynowania (s. 386).

Wykaz danych jest fizycznie przechowywany w plikach wykazu. Każdy skarbiec korzysta z własnego zestawu plików wykazu, które znajdują się zwykle w samym skarbcu. Jeśli nie jest to możliwe, jak w przypadku urządzeń taśmowych, pliki wykazu są przechowywane na komputerze zarządzanym lub w folderze lokalnym węzła magazynowania. Węzeł przechowywania zawiera również zapisane lokalnie pliki wykazu jego zdalnych skarbców, co zapewnia szybki dostęp do zgromadzonych w nich danych.

Z

Zadanie

Zestaw czynności przeznaczonych do wykonania przez program Acronis Backup & Recovery 11 w określonym czasie lub po wystąpieniu określonego zdarzenia. Są one opisane w pliku usługi w formie nieprzeznaczonej do odczytu przez użytkownika. Czas wystąpienia lub zdarzenie (harmonogram) jest przechowywane w chronionych kluczach rejestru (w systemie Windows) lub w systemie plików (w systemie Linux).

Zadanie lokalne

Zadanie (s. 388) utworzone na komputerze zarządzanym (s. 380) przy użyciu funkcji zarządzania bezpośredniego (s. 389).

Zadanie scentralizowane

Zadanie (s. 388) rozsyłane do komputerów z serwera zarządzania (s. 384). Zadanie takie można modyfikować jedynie w drodze edycji oryginalnego zadania lub scentralizowanego planu tworzenia kopii zapasowych (s. 384) na serwerze zarządzania.

Zarządzanie bezpośrednie

Operacja wykonywana na komputerze zarządzanym (s. 380) przy użyciu bezpośredniego połączenia konsola (s. 380)-agent (s. 376) (w przeciwieństwie do zarządzania scentralizowanego (s. 389), w którym operacje są konfigurowane na serwerze zarządzania (s. 384) i przekazywane z serwera na komputery zarządzane).

Operacje zarządzania bezpośredniego:

- tworzenie lokalnych planów tworzenia kopii zapasowych (s. 381) i zarządzanie nimi;
- tworzenie zadań lokalnych (s. 388), takich jak zadania odzyskiwania, i zarządzanie nimi;
- tworzenie skarbców osobistych (s. 385) i przechowywanych w nich archiwów oraz zarządzanie nimi;
- wyświetlanie stanu, postępu i właściwości zadań scentralizowanych (s. 389) istniejących na komputerze;
- przeglądanie dziennika operacji agenta i zarządzanie nim;
- operacje zarządzania dyskami, takie jak klonowanie dysku oraz tworzenie i konwertowanie woluminu.

O swego rodzaju zarządzaniu bezpośrednim można mówić w przypadku korzystania z nośnika startowego (s. 381).

Zarządzanie scentralizowane

Zarządzanie infrastrukturą Acronis Backup & Recovery 11 za pośrednictwem centralnej jednostki zarządzania pod nazwą Acronis Backup & Recovery 11 Management Server (s. 384). Do operacji zarządzania scentralizowanego zalicza się:

- tworzenie scentralizowanych planów tworzenia kopii zapasowych (s. 384) dla zarejestrowanych komputerów (s. 380) i grup komputerów;
- tworzenie statycznych (s. 379) i dynamicznych grup (s. 378) komputerów (s. 380) oraz zarządzanie nimi;
- zarządzanie zadaniami (s. 388) istniejącymi na komputerach;
- tworzenie skarbców centralnych (s. 385) do przechowywania archiwów i zarządzanie nimi;
- zarządzanie węzłami magazynowania (s. 386);
- monitorowanie działania komponentów programu Acronis Backup & Recovery 11, tworzenie raportów, przeglądanie centralnego dziennika itd.